Procurement of an EHR solution with adjacent systems and services

***

Invitation to Dialogue

Appendix C1 Customer Technical Platform

Case number: 2016/238

History

Version	Responsibility	Date	Comments/Changes
v1.0	Helseplattformen	02.02.17	Version v1.0 shared with the Contractors

Content

Tables

Figures

List of Annexes

Annex 1 - Application list

1 INTRODUCTION

This Appendix provides an overall description of the technological components and infrastructure that comprise the Customer's platform as of February 2017. Expected changes for the Customer's platform are described in *Appendix C7*.

For a successful implementation and operation of the EHR solution, it is essential that the parties have a common understanding of what is described in this Appendix, and that any significant constraints and limitations are disclosed and taken into account by the parties.

Requirements for the solution in terms of general, functional, technical and maintenance requirements are described in *T Appendix 1A, T Appendix 1B, T Appendix 1C* and *V Appendix 1*.

Note that in general, all deliveries and pre-requisites or assumptions relevant for the implementation of the EHR solution, both related to the Contractor's Deliverables and the Customer Furnished Assets (CFA), cf. *Appendix C7,* shall be taken into account in the Contractor's Project and Progress Plan, cf. *T Appendix 3*.

1.1 GLOSSARY

Terms and expressions with capital letters shall have the meaning set out in *Appendix C4*. Terms marked with ***bold, italic font*** are terms that the Customer has wished to provide an explanation of to ensure a common understanding, cf. *Appendix C4.* These terms and definitions should be interpreted in the context of this specific procurement, and are not intended to be general definitions beyond this scope. The terms are in addition to cf. *Appendix C5, Annex C – Glossary of Terms for EHR-S FM*.

2 OVERVIEW OF INFRASTRUCTURE, APPLICATIONS AND INTEGRATIONS

This Chapter describes the national infrastructure that the solution has to operate within. Some of the figures show the complexity of the information exchange and integrations between systems and actors.

2.1 THE NORWEGIAN HEALTH NETWORK

The ***Norwegian Health Network (NHN)***, owned by the Ministry of Health and Care Services, is the public infrastructure for the sharing and exchange of health-related information between the different users and actors in the Norwegian health sector. The NHN makes it possible for these parties to carry out their respective tasks in a secure and effective manner. In addition, the NHN manages and supplies national services, such as national portal services, national health and administrative registries. All parties declare a mandatory compliance with a certain technical and security configuration level before they are connected.

Figure 1 shows the Norwegian health service's main actors and their interconnection.

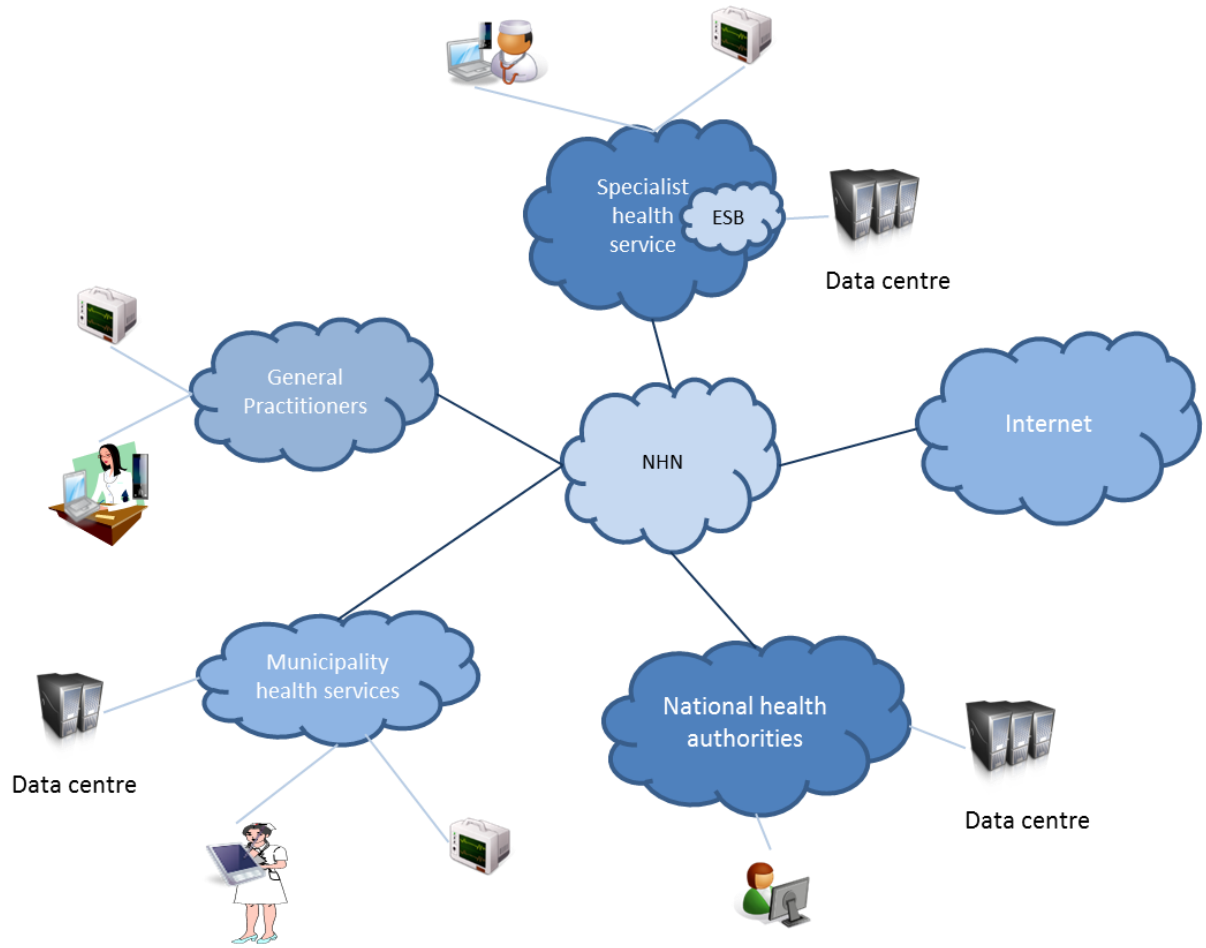


Figure 1 - Health services interconnection overview

The specialist health service comprises hospitals, which provides laboratory services, ***emergency medical communication centres,*** amongst other services.

Municipal health services and ***GPs*** also connect to the ***NHN*** to be able to interact with the National collaboration framework, specialist health services, national health authorities and other GPs.

None of the actors have direct access to internet. The different actors get their internet access through the NHN who provides a secure internet connection. An exception to this is the municipalities that maintain their own separate internet connection through ISP providers.

2.2 SPECIALIST HEALTH SERVICE EHR INTEGRATIONS

Figure 2 shows an overview of the information exchange between the EHR systems in the Central Norway Health Region, other application domains in the specialist health service, the municipal health service in the Central Norway Health Region and other external actors in the health service.

The focus is the EHR system in the specialist health service. The figure does not give an exhaustive list of applications or information exchange, but gives an impression of the complexity of the information exchange. Some of the text in this figure is in Norwegian.

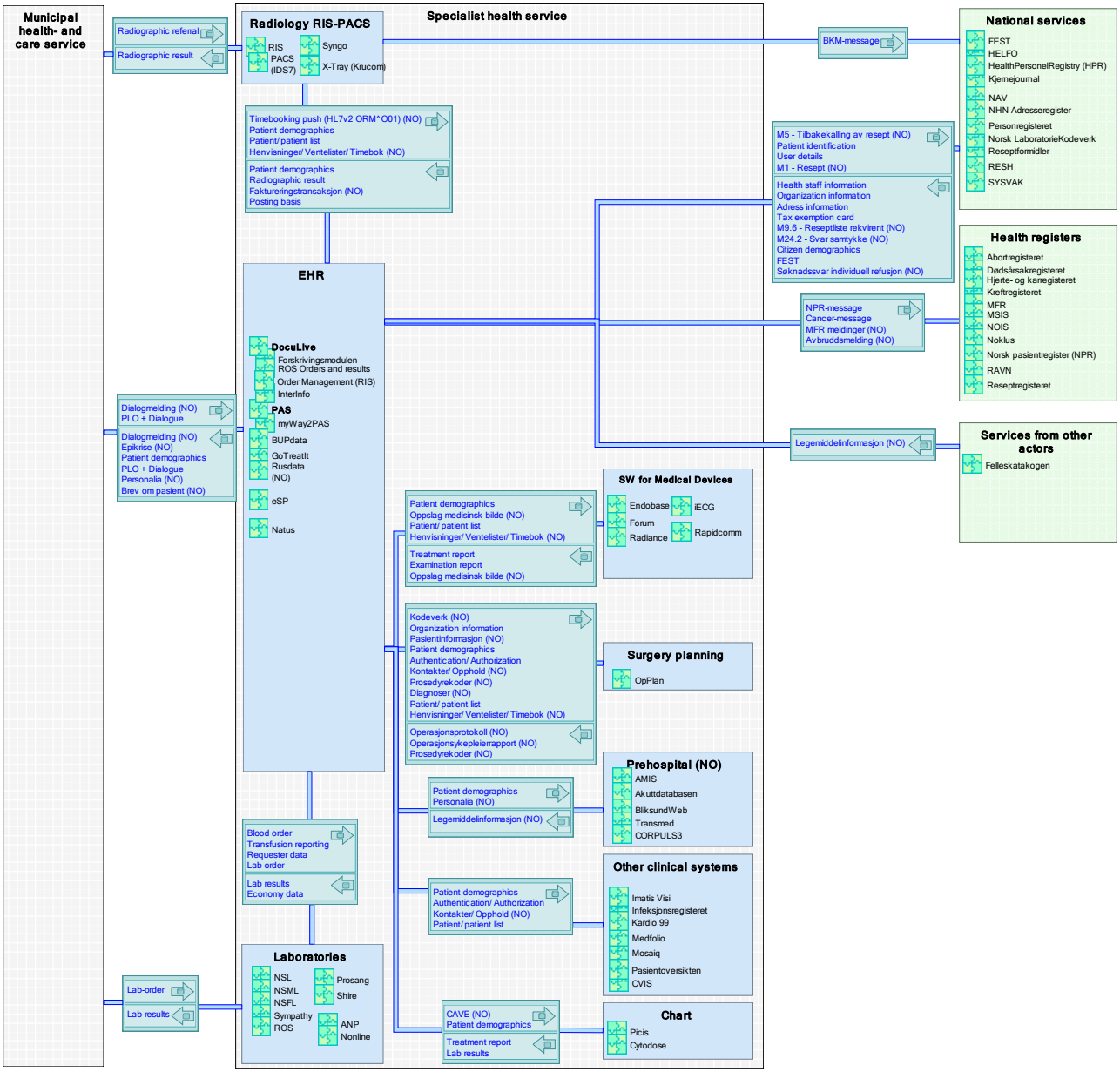


Figure 2 - Overview of integrations within the specialist health service, municipal health service and national services (not exhaustive)

2.3 MUNICIPAL NURSING AND CARE SERVICE EHR INTEGRATIONS

Figure 3 shows an overview of the information exchange between the EHR systems in the municipal nursing and care service, specialist health service, GPs and other external actors in the health service.

The focus is the EHR systems in the municipal nursing and care service. The figure does not give an exhaustive list of application or information exchange, but provides an impression of the complexity of the information exchange. Some of the text in this figure is in Norwegian.

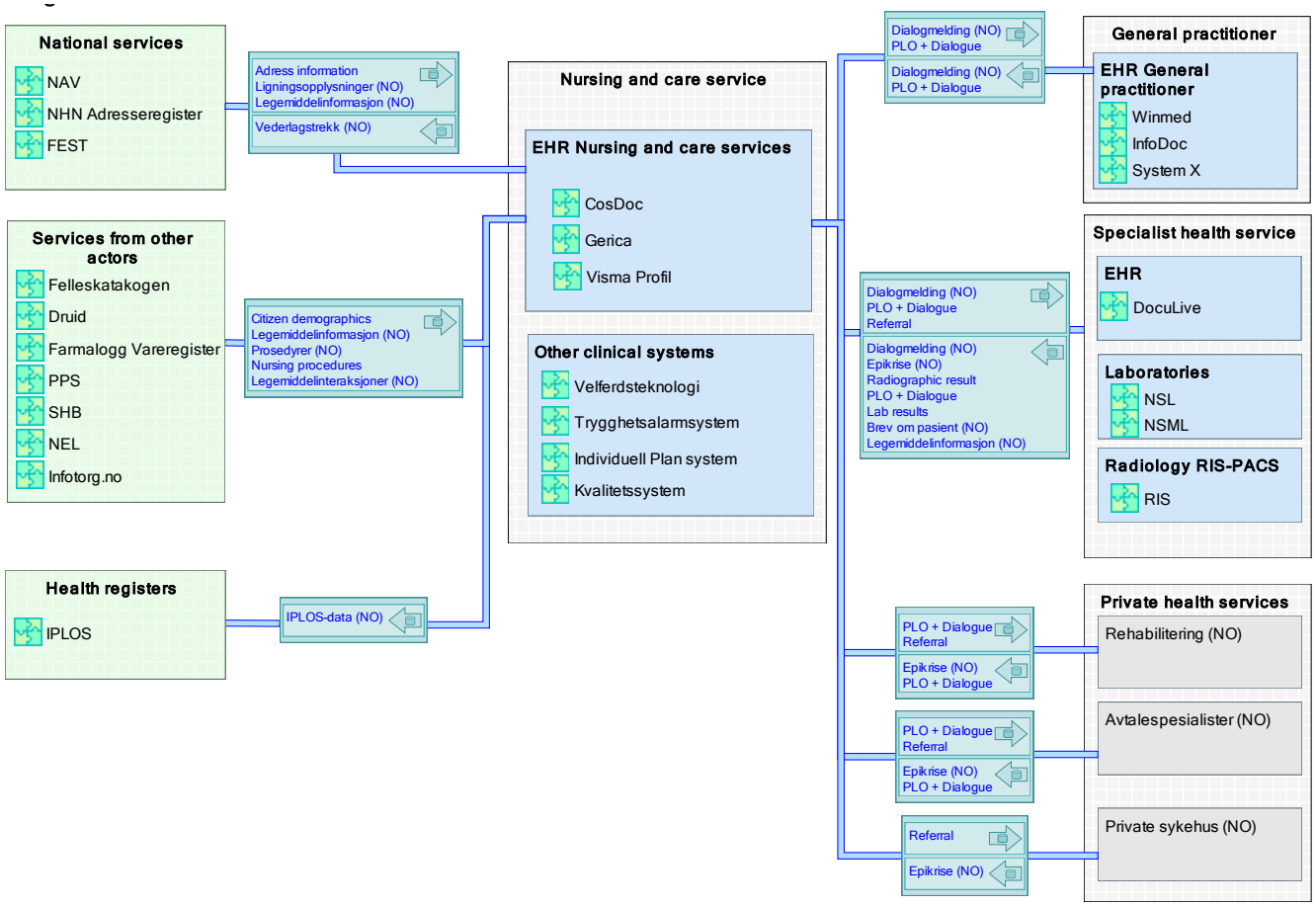


Figure 3 - Overview of integrations with the municipal nursing and care services' EHR systems (not exhaustive)

2.4 GENERAL PRACTITIONER EHR INTEGRATIONS

Figure 4 shows an overview of the information exchange between the GPs' EHR systems, specialist health services, municipal nursing and care services and other external actors in the health service. The focus is the GPs' EHR systems.

The figure does not give an exhaustive list of applications or information exchange, but provides an impression of the complexity of the information exchange. Some of the text in this figure is in Norwegian.

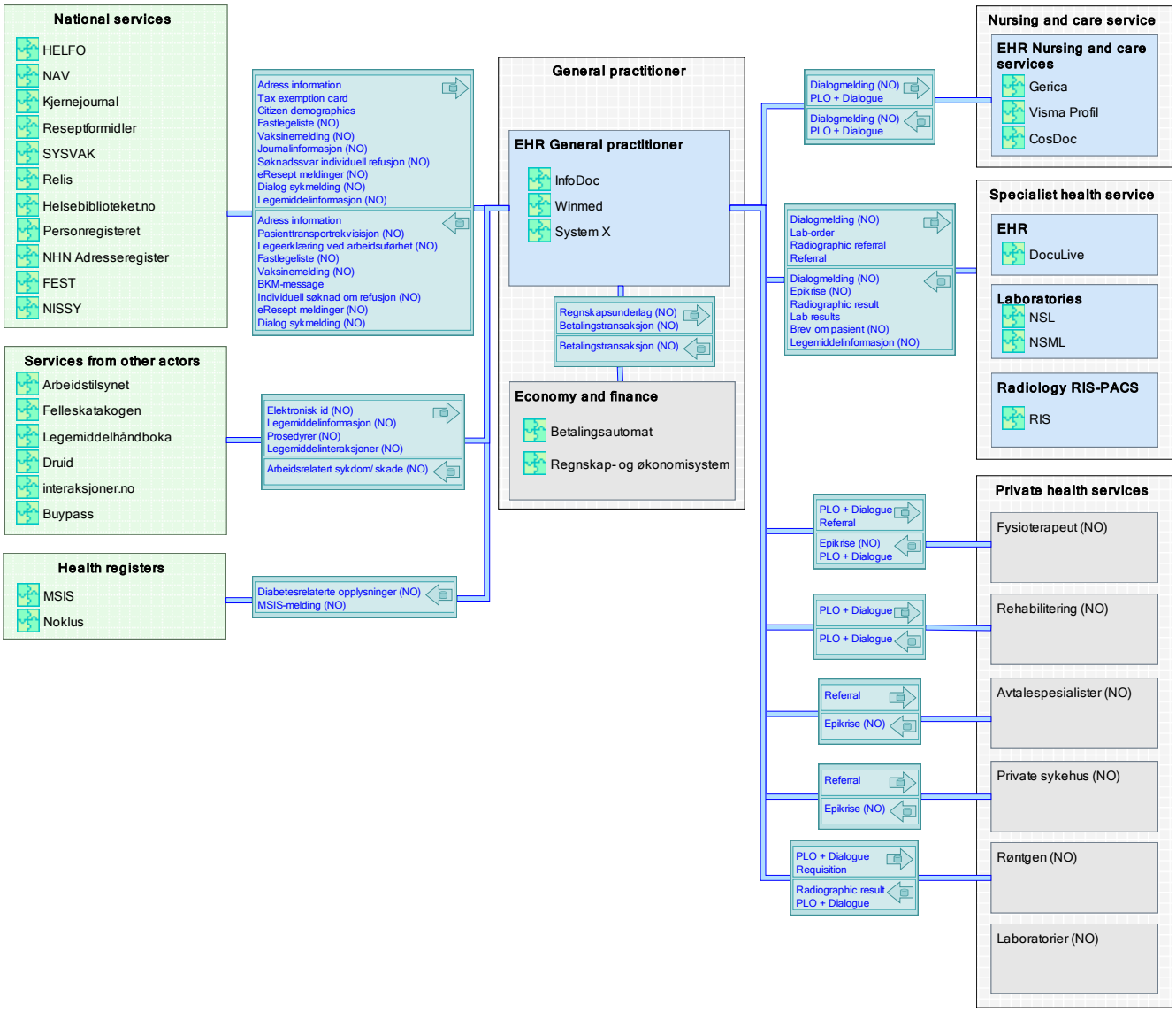


Figure 4 - Overview of integrations with the General practitioners' EHR systems (not exhaustive)

2.5 APPLICATIONS

This Chapter provides a list of applications to be replaced by and integrated with the new EHR solution. The applications are listed in alphabetic order and are used by municipalities and specialist health service (hospitals). In addition, the following application attributes are listed:

- The application name
- A short description of the application
- Municipalities/hospitals - indicating where the application is used
- Supplier
- The application domain
- Speciality - indicating which medical speciality uses the application

The applications are listed in *Appendix C1, Annex 1.*

3 TECHNICAL PLATFORM SPECIALIST HEALTH SERVICE

The scope of this Chapter is to describe the technical infrastructure for the specialist health service, except applications and systems, as they are described in *Annex 1*. The objective is to give a technical description of the current technical infrastructure, the operational environment supporting the current EHR and their closest surroundings.

3.1 OVERVIEW

This Chapter describes the interconnected internal business organisations, the integrated external organisations, the integration services and the external services. As a supplement, some operational facts about the current EHR system are described.

Figure 5 below shows how the hospitals in the different counties interconnects through wide area network (WAN) connections (medium blue clouds) and connects to the national health authorities, municipalities and internet (dark blue clouds) through the ***NHN*** connection (light blue cloud). The ***enterprise Service Bus*** (***ESB)*** (light blue cloud) orchestrates message exchange between the specialist health service and the municipalities.

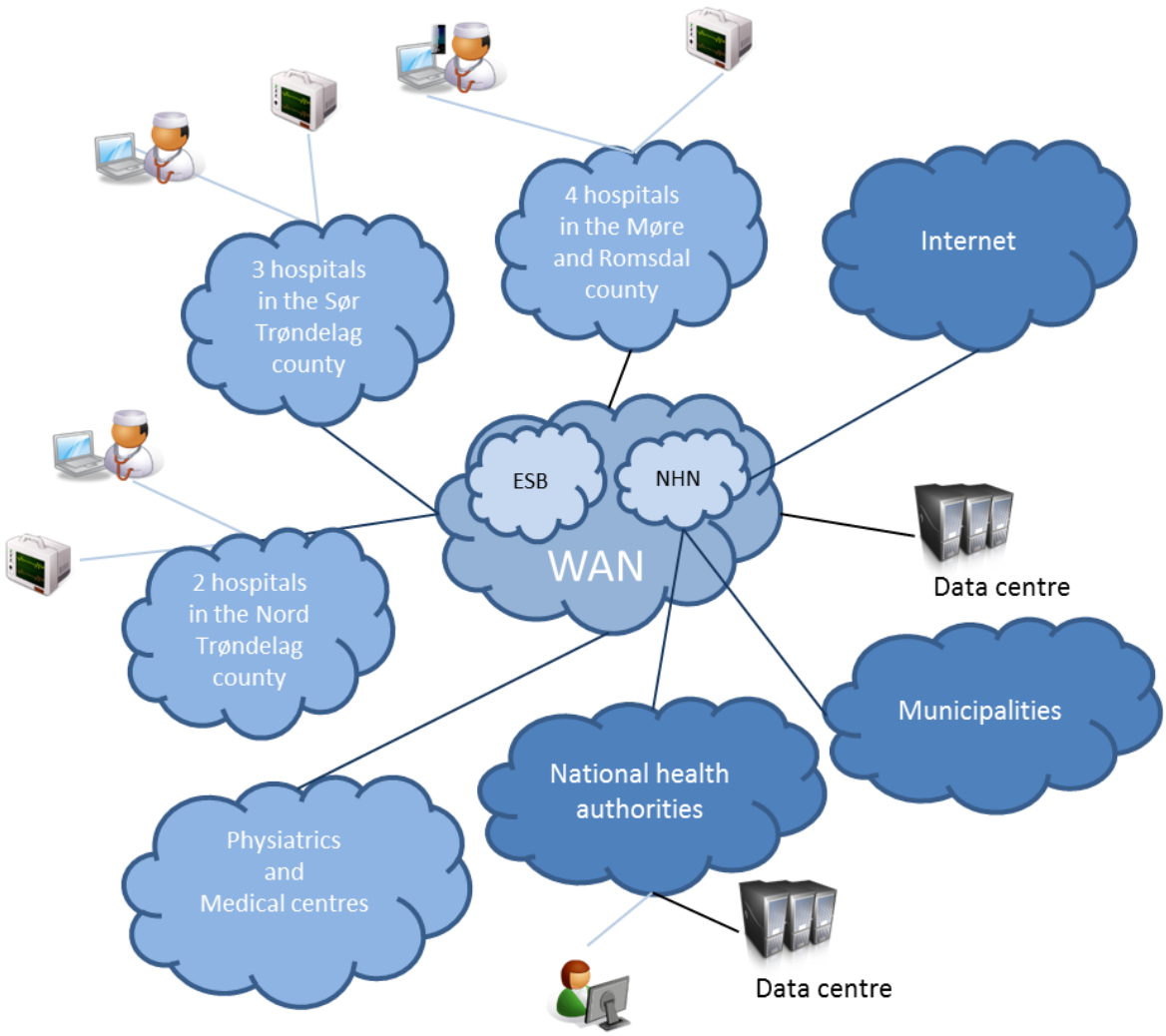


Figure 5 - Overview of the specialist health service

A high availability data centre, physical distributed on two different physical locations in Trondheim, provides the technical infrastructure necessary to expose shared health services to the other actors in the health sector.

Table 1 below shows some operational facts for the current ***EHR*** system, ***Doculive***, serving the specialist health service.

Table 1 - Operational facts

Object	Facts
PULS and SPRINT PC clients (See chapter 3.8)	Approximately 16,000 physical PULS clients and 3,000 SPRINT (VDI) managed clients (cf. *Chapter 3.8)* summing up to the total of 19,000. Approximately 1,800 concurrent users are using SPRINT VDI clients during working hours.
Doculive users (present EHR solution)	A total of 27.797 Doculive users are defined. 10,948 different users were logged on in November 2015
Doculive client application	The client application is installed on 6,000 physical PULS clients due to requirements for voice recognition, local connected scanners and other local devices. The client application is streamed (APP-V) to the remaining physical PULS and SPRINT clients (VDI).
Doculive server platform	The server platform comprises Windows server 2008 R2 Enterprise. The database platform is Microsoft SQL 2008 R2.
Doculive database storage volume	The grand total health record storage volume is 3.3 TB. The storage volume of the largest database table is 1.05 TB, storing 1,967,838,778 rows. The total storage volume for scanned graphical documents is 50 TB.

Table 2 below shows the number of database records managed by Doculive, serving 1,605,546 patients.

Table 2 - Doculive database records

Record category	Number of records
Written records	65 210 437
Scanned records	26 058 998
Voice recording records	3 393 380
New records in November 2015	624 169
New records in 2015	6 607 910

Table 3 below shows number of clinical Laboratory prescriptions every year since 1989.

Table 3 - Clinical laboratory prescriptions

Year	Prescriptions
1989	351
1990	301 233
1991	571 351
1992	771 081
1993	840 381
1994	855 714
1995	913 418
1996	997 842
1997	1 008 139
1998	990 268

1999	1 016 107
2000	1 080 611
2001	1 131 493
2002	1 173 657
2003	1 233 622
2004	1 273 164
2005	1 336 371
2006	1 375 058
2007	1 337 331
2008	1 352 130
2009	1 330 886
2010	1 314 704
2011	1 327 737
2012	1 373 629
2013	1 423 658
2014	1 449 108
2015	1 404 058
Total	**29 183 103**

Table 4 below shows number of microbiological laboratory prescriptions every year since 1989.

Table 4 - Microbiological laboratory prescriptions

Year	Prescriptions
1990	8 1961
1991	248 005
1992	248 856
1993	276 441
1994	268 980
1995	262 899
1996	268 584
1997	271 691
1998	272 772
1999	277 814
2000	283 382
2001	289 816
2002	301 112
2003	297 000
2004	300 993
2005	309 683
2006	290 449
2007	270 206
2008	274 773
2009	280 526
2010	264 335
2011	283 549
2012	276 676
2013	281 345
2014	304 353
2015	291 452
Total	**7 077 653**

3.2 NETWORK

This Chapter describes the different types of networks interconnecting with the technical infrastructure, the network protocols used and the control mechanisms managing the traffic flow.

3.2.1 Wide Area Network (WAN)

The WAN infrastructure comprises a large number high capacity and redundant leased lines (fibre and other technologies) from different communication vendors in the market. Line capacity and redundancy varies from site to site according to the size of the organisation to interconnect.

A high capacity NHN connection provides a secure and functional electronic message exchange with the other actors in the health sector and a secure internet connection.

Cisco technology forwards and routes the IP-based network traffic between sites in the health service.

3.2.2 The Norwegian Health Network (NHN)

The NHN, owned by the Ministry of Health and Care Services, interconnects the Norwegian health sector and supplies common application services as well as an internet connection to the connected participants.

3.2.3 The Local Area Network (LAN)

The LAN infrastructure comprises high capacity lines (1 GB or higher) and the local network traffic are routed and forwarded by Cisco technology, based on a standard edge, distribution and core layered switch architecture.

Cisco edge switches are of type WS-3560, WA-3560E and WS-C4500-E. Cisco core switches/routers are of type WS6500 and Nexus7000.

3.2.4 Wireless Local Area Network (WLAN)

Wireless networks are available throughout the specialist health service and the managed clients do an automatic connection to the uniform and enterprise wireless network name (SSID). A guest wireless network is also available for unmanaged clients.

The wireless network infrastructure comprises solely of Cisco technology, implemented as a centralised architecture, giving the central high-available master Wireless LAN Controllers (WLC) the mandate to control the distributed slave access points (AP).

Managed PC clients have to perform a successful IEEE 802.1x machine authentication to get access to wireless networks.

Cisco APs are of type Aironet 3700,3600,3500,1242 and the WLCs of type Cisco WiSM.

3.2.5 Virtual Local Area Network (VLAN)

Virtual LANs partitions the physical network into different logical network zones. The network traffic flows in a physical network infrastructure partitioned in different logical network zones, to ensure a secure and functional handling and transport of different information classes.

PC clients get access to logical networks zones by performing a successful IEEE 802.1x authentication and a dynamic VLAN assignment.

Figure 6 below shows how different VLANs partitions the network into different logical network zones.

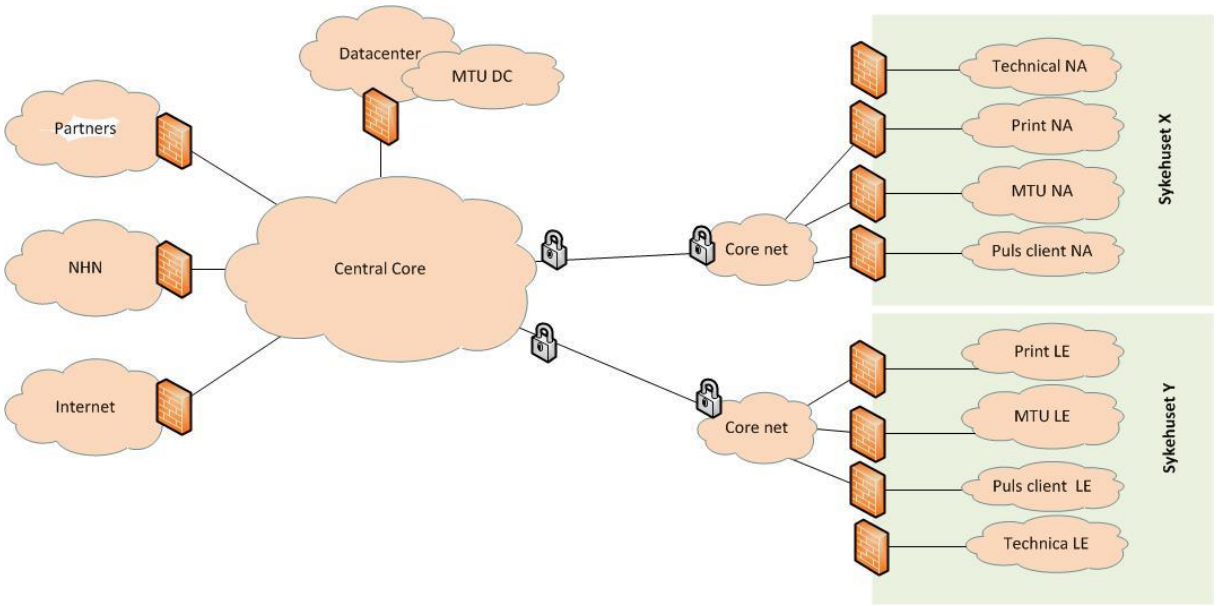


Figure 6 - Virtual LAN

3.2.6 Firewall

Firewalls are managing and controlling the IP network flow, ensuring an intended network flow between logical network zones. A central management station are managing and distributing the firewall rules.

All network traffic forwarded through and blocked by the Firewall is logged.

The Firewall technology is mainly Cisco ASA on WISM module and Check Point.

3.2.7 Remote access

Remote access for employees in the specialist health service uses Microsoft Direct Access, which requires support for IP version 6.

A Citrix-based remote access solution enables remote access for ***administrators*** and suppliers.

3.2.8 Protocols

The basic communication protocol is IP version 4.

3.3 APPLICATION ENVIRONMENT

This Chapter describes the infrastructure components and tools providing the production environment for applications and application services.

3.3.1 Virtual servers

The specialist health service have standardised on virtualised hardware and the grade of virtualisation is more than 90 per cent (about 1300 servers). Windows servers are running on VMWare ESXI.

3.3.2 Virtualisation technology

Figure 7 shows the distribution of VMware farms on the different hospitals in the health region.

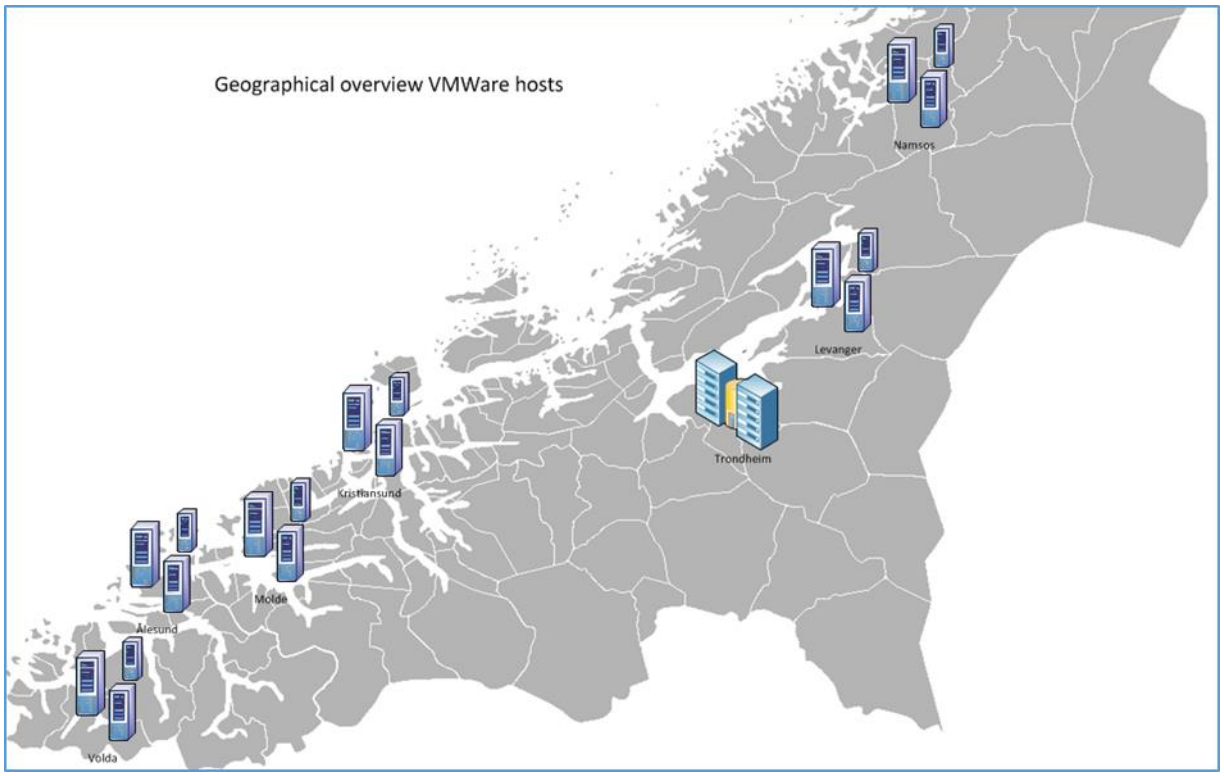


Figure 7 - Server virtualisation

The production environment comprises several VMware farms located at the hospitals, in different geographical locations. The VMware farms comprises a total of 50 ESXi hosts and approximately 30 of them are located at the main datacentre in Trondheim.

A VMware VDI farm comprises 64 ESXi hosts scaled to publish approximately 6.000 virtual clients.

3.3.3 Physical servers

Several physical HP NonStop servers (former Tandem Computers) run the patient administrative system, laboratory systems and a shared authentication solution for several other systems.

SQL servers running consolidated databases are running on physical server hardware due to extensive workload.

3.3.4 Operating systems

The standard server operating system is Microsoft Windows servers, version 2008 R2 and 2012 R2.

HP NonStop servers are running NonStop operating system.

Web servers are mainly Microsoft Internet Information Server (IIS) version 7.5 and 8.5.

3.3.5 Database

The specialist health service is standardising on Microsoft SQL servers configured as a Failover Clustered environment, comprising of several database instances in each cluster. The different SQL instances support a consolidated production environment.

Separate SQL instances or dedicated physical/virtual database server are allocated for systems with special needs or extensive workload.

A few databases are running on Oracle ver. 12c RAC. Oracle is running on top of Windows server 2012 R2.

Database for laboratory systems and patient administrative system are running on HP NonStop servers.

3.3.6 Anti-virus

Windows servers are running Trend antivirus software and the Windows firewall is enabled.

3.3.7 Backup

Snapshot technology performs backup and restore of data in the VMware environment. Accordingly, NetBackup performs backup and restore of data on physical servers.

Backup and restore of databases are performed by RMAN for restore Oracle databases and SQL agent job (T-SQL) on file share (Data Domain) for Microsoft SQL databases.

3.3.8 Monitoring

A dedicated team is developing and maintaining monitoring solutions for servers and network.

3.3.8.1 Network

SPLUNK monitors data traffic by performing correlation of logs from network and firewall devices, to detect issues. SPLUNK is also used to create monitoring dashboards for different services.

Network Node Manager (NNM) monitors all network nodes, both wired and wireless.

Cacti is used to monitor and log network traffic and load.

NeDi keeps track of the relationships between VLANs, switch ports and connected nodes.

Websense monitor and control web traffic.

3.3.8.2 Server

SPLUNK monitors services by performing correlation of logs from servers, to detect incidents.

Foglight performs real time monitoring and trending of VMWare environments.

Spotlight performs real time monitoring of database servers and SQL instances.

A self-made database monitoring-solution, customises monitoring, reporting and trending of databases.

Microsoft System Center Operations Manager (SCOM) is the standard monitoring suite for servers. SCOM is custom configured to fit different needs for monitoring of services and systems. Dashboards are used to display customised heat maps for different monitoring needs suited for different purposes.

The Riverbed performance management suite performs monitoring, debugging and trending of network traffic and performance related issues.

3.3.9 Software distribution

Patching and updating of servers follow Microsoft best practise. Microsoft System Center Configuration Manager (SCCM) performs automated server patching.

Automated SCOM functionality patches approximately 90% of the servers and the remaining servers are patched manually.

3.4 INFRASTRUCTURE SERVICES

This Chapter describes the infrastructure services used by applications to authenticate and authorise users, and to distribute electronic mails.

3.4.1 Active Directory (AD)

Microsoft Active Directory forest contains ten domain controllers with functional level 2008 R2. The domain controllers are running on Windows server 2008 R2 and 2012 R2.

Four of the domain controllers are located at the datacentre in Trondheim. The remaining domain controllers are located at the other hospitals in the health region.

AD is a shared directory containing different objects (e.g. users, user groups, clients, servers). User logs on to the shared user directory and is granted access to resources defined in the Windows domain.

Figure 8 below shows the distribution and locations of AD domain controllers in the Windows domain *Helsemn.no* serving the specialist health service.

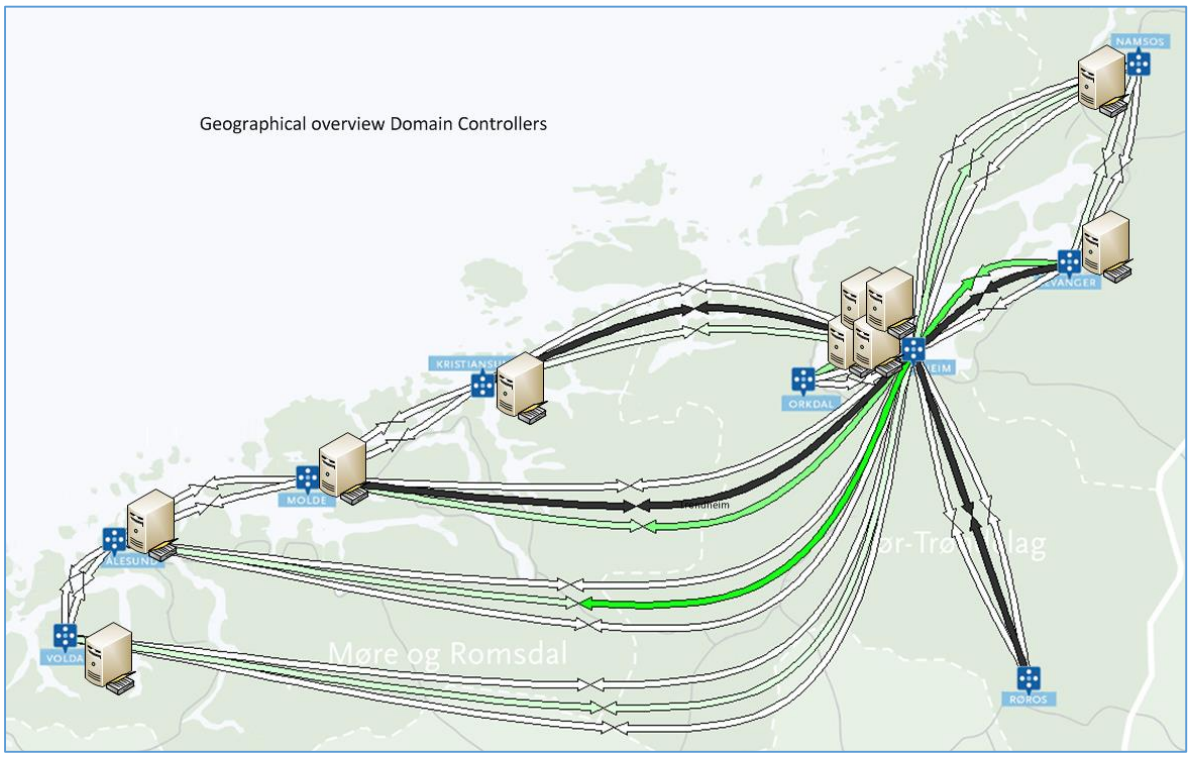


Figure 8 - Active Directory

3.4.2 Active Directory Federation services (ADFS)

ADFS is implemented to enable access to remote web application services for local users and access to local web application services for remote users.

3.4.3 PKI

An intermediate PKI service issues certificates to clients, servers and users.

The ***NHN*** is hosting the root CA and the revocation information is published in the ***NHN*** network. The Microsoft AD CS intermediate CA is managed by the specialist health service and the local revocation information is published in AD and to a Certification Revocation List (CRL) web server.

3.4.4 Email service

The email solution is Microsoft Exchange 2010 SP2, running on Windows server 2008 R2 virtualised server infrastructure.

Figure 9 shows the high availability email service configuration for the MS Exchange email system. The basic email service infrastructure is divided and serves the email service from two physical datacentres.

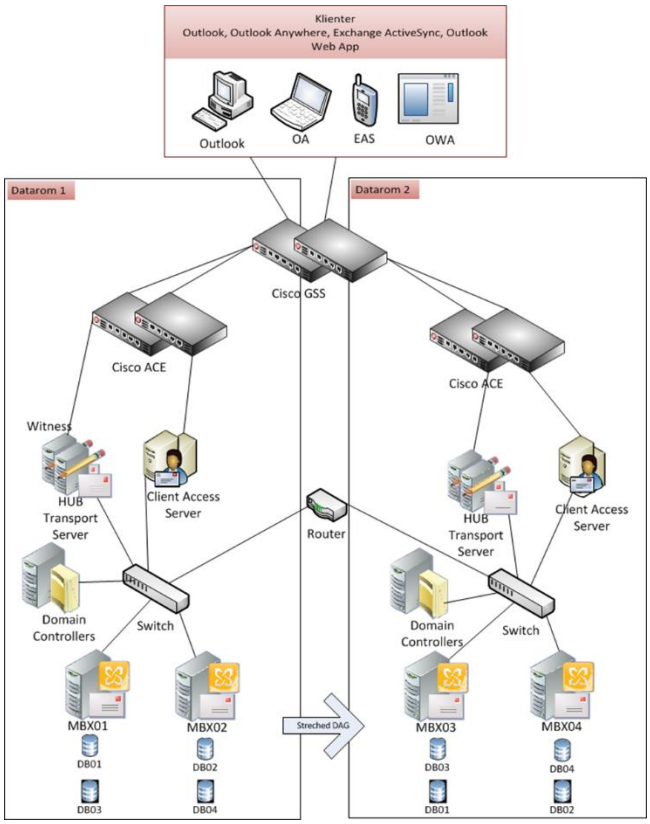


Figure 9 - Email service

3.5 STORAGE AREA NETWORK (SAN)

This Chapter describes the general purpose for mid and high-end quality data storage services.

The high-end quality storage solution Hitachi VSP G1000, is configured with a synchronous mirroring between datacentres over a dedicated fibre network.

Figure 10 shows the high-end quality storage solution implemented in two physical datacentres. Updates to either of the SAN nodes will be mirrored to the other node.

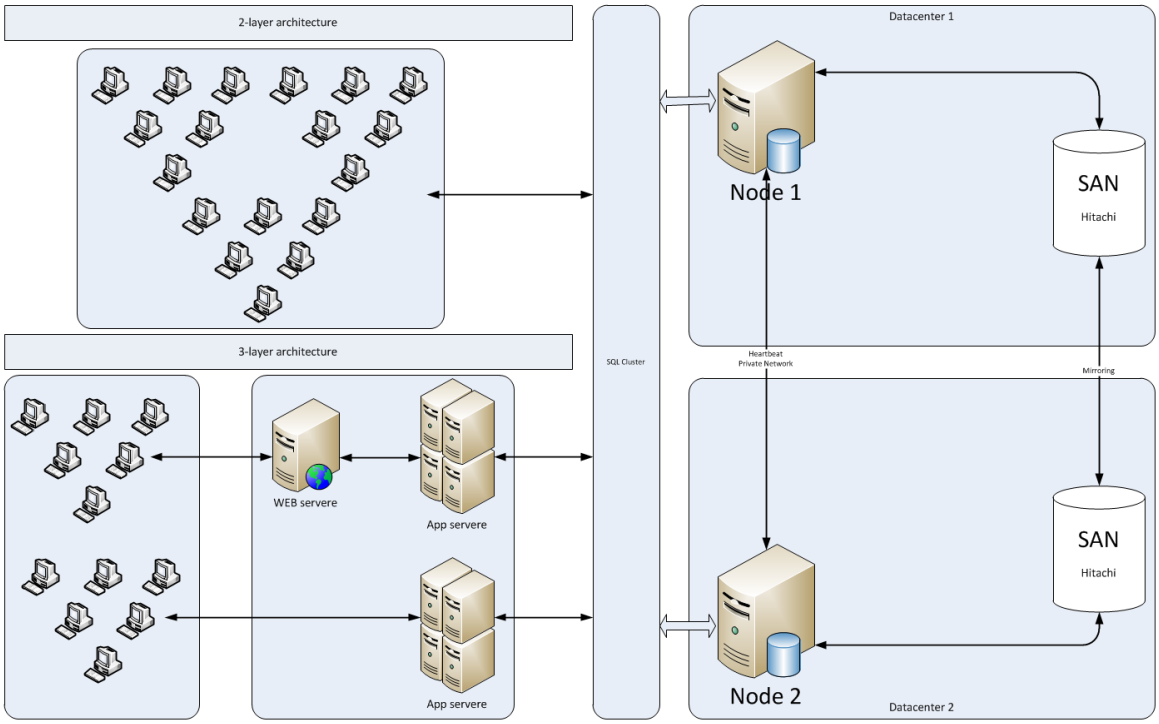


Figure 10 - High-end SAN

The mid-range quality storage solution is NetApp SAN configured with asynchronous mirroring every hour over a dedicated fibre network.

Figure 11 shows the mid-range quality storage solution implemented in two physical datacentres. Updates to either of the SAN nodes will be mirrored to the other node asynchronously every hour.

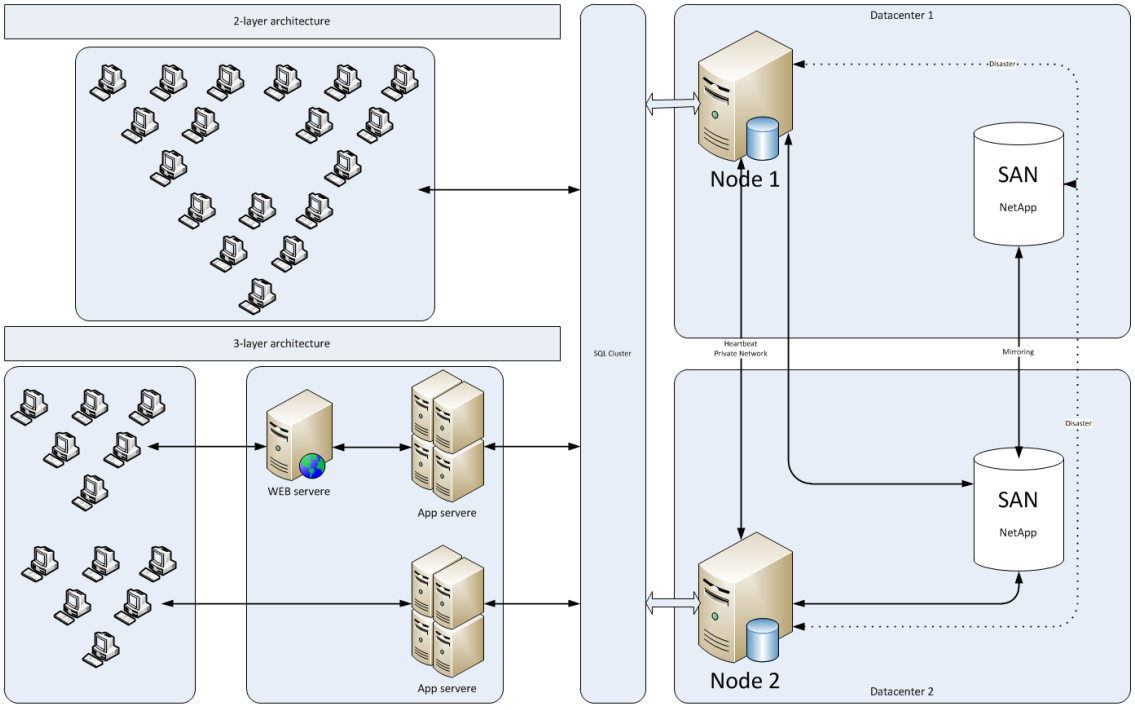


Figure 11 - Mid-range SAN

Data Domain from EMC is used as backup storage, currently running DD2500 and DD670.

3.6 AUTONOMOUS SUBSYSTEMS

This Chapter describes the integration system exchanging information with other parts of the health sector and the data warehouse for health management and development.

3.6.1 Data warehouse

Figure 12 below gives an overview of one of the current data warehouse solutions.

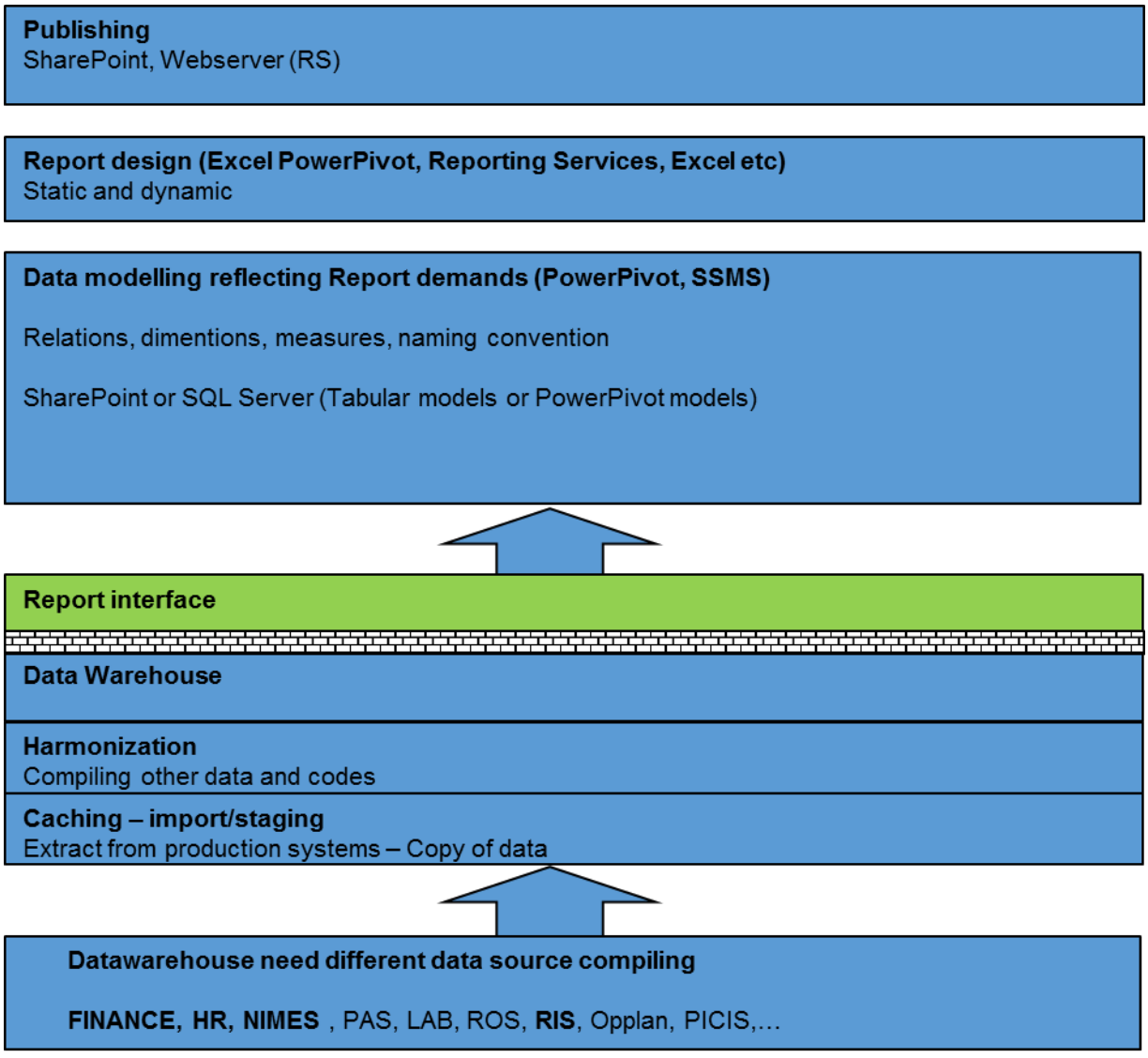


Figure 12 - Data warehouse

Report interface basic information (marked green) is extracted from various backend systems.

3.6.2 Integrations

Figure 13 below shows the message exchange between the different actors and between the actors and national registers/health authorities.

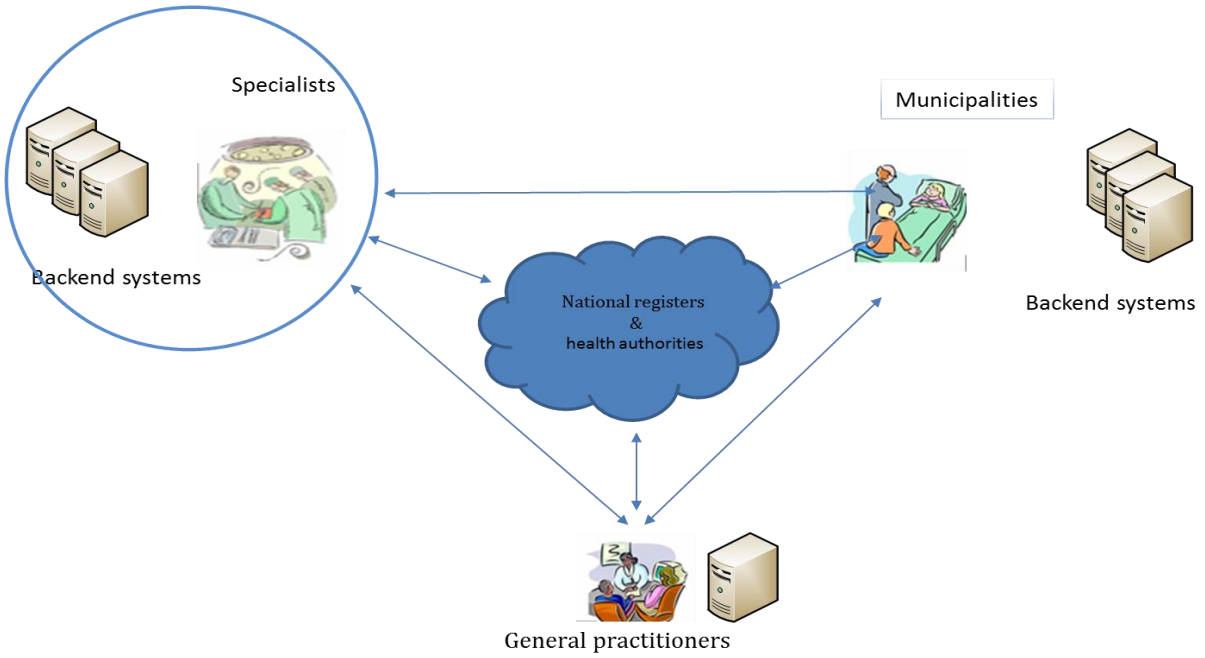


Figure 13 - Integration overview

The ***enterprise service bus (ESB)*** comprises among others a Microsoft BizTalk 2013 R2 integration service, orchestrating internal and external integrations. The latter ones (the blue square in Figure 14 below) integrate the health authorities, municipalities, ***general practitioners (GP)*** and partners/actors in other health regions in Norway, with the specialist health service in HMN.

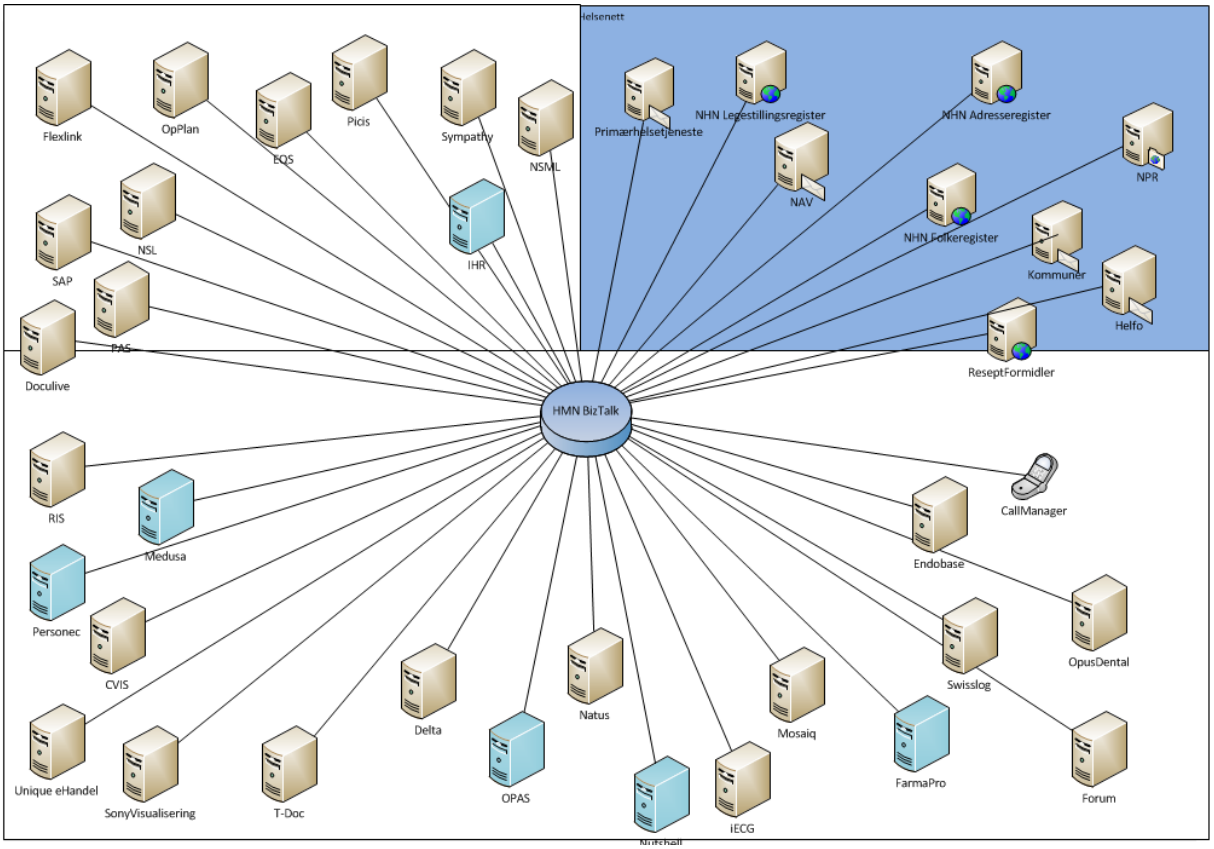


Figure 14 - Internal and external integrations

Internal integrations provide data exchange and transformation utilising Netapp File Transfer, SQL, MSMQ and Web services.

External integrations provide data exchange and transformation utilising SMTP/POP3, FTP/SFTP and Web services.

Table 5 – Examples of external integrations

Sender	Receiver	Message Content	Comment
PAS	NAV/***The Norwegian Health Economics Administration (Helfo)***	BKM (refunds)	National format
Doculive	Reseptformidleren (national prescription)	Prescription refund	National format
GP	Specialist health services	IHR Request	National format

3.7 CONTINUITY

This Chapter describes the stand-by solutions to be used in an emergency situation.

The current Doculive ***EHR*** system Microsoft SQL Failover Cluster is running on dedicated physical servers installed in a third physical datacentre in Trondheim.

In an emergency situation, where the main datacentre is out of service, a read-only copy of the database is available in the third datacentre.

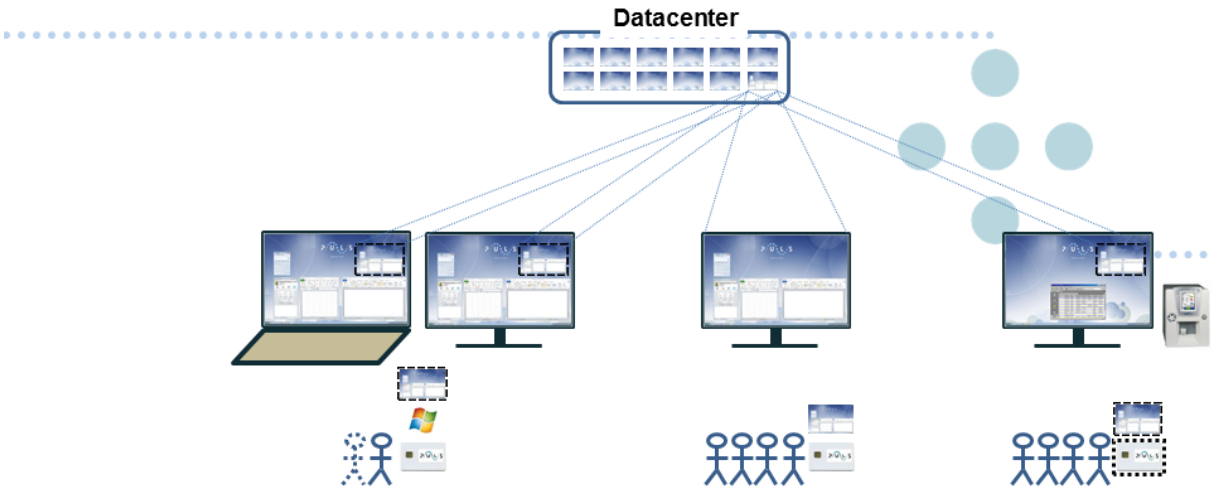
The database is during normal operation updated with log shipping and the logged transactions are executed with a delay of approximately two hours.

3.8 CLIENTS

This Chapter describes the different client types, the hardware and basic software dependencies, and the client application configuration and distribution.

PULS is the name of the in-house developed concept for PC configuration and management. There are defined three different types of the PULS clients:

- Standard
  - Standard Windows 7 client intended for regular clinical and administrative use, where the users log on using a personal smart card. These types of clients are typically used where there are only one or two users sharing a computer, for example in an office.
- Special
  - Standard Windows 7 client with automatic system user logon at startup intended used for clients with ***medical devices*** connected or applications with special requirements.
- Sprint
  - Locked down Windows 7 installation, used as thin client endpoints for the Virtual Desktop Infrastructure (VDI). These clients are typically used where there are multiple users sharing the computer, for example in the clinics and wards. Users log on/reconnect using a personal smart card and disconnects from the session when the smart card is removed.



PC Client	Standard	Sprint (VDI)	Spesial
Locally installed applications	Yes	No	Yes
Virtualized applications	Yes	All	Yes
Windows local logon	Smartcard	N/A	Automatic with system user
Windows logon to VDI	Smartcard	Smartcard	Smartcard
Windows reconnect to VDI	Smartcard	Smartcard	Smartcard
When removing smartcard	Lock/Logoff desktop	Disconnect	Disconnect VDI
Mobility	Laptop with DA/VPN	N/A	N/A
Offline functionality	Offline Files and local mail	N/A	N/A

Figure 15 - Characteristics of the different PULS client types

The Virtual Desktop Infrastructure (VDI) is offered on a VMware Horizon View platform and is scaled for 4,000 concurrent users. VDIs are mainly used by clinical users with the need to log on to multiple computers on multiple locations during a working day. By disconnecting/reconnecting to the virtual desktops, they save time and get to keep their session when they move from computer to computer.

Desktop pools are floating linked clones that refreshes once a week. Golden image is a Windows 7 installation, with a minimum set of basic applications and middleware installed, and best practice tuning for running in a VDI environment.

Laptops use a local user profile and have enabled a functionality for offline sync of documents and email. Remote access for PULS clients are provided by Microsoft Direct Access.

Clients are running System Center Endpoint Protection and the local Windows Firewall is enabled, centrally managed via Group Policy (GPO). PC clients are patched on a monthly basis (Windows, Office, Adobe Flash, .Net, Silverlight, AV, IE) and virtual clients once every third month.

3.8.1 Basic Software

The centrally managed clients are based on a Microsoft SCCM distributed client image and Active Directory Group Policy (GPO) configuration.

The following software is a part of the image, and available from all types of clients:

- Microsoft .Net Framework 4.5.2

- Microsoft Silverlight 5.1.4
- Microsoft Office 2010
- 7-Zip 9.20
- Adobe Flash Player (IE) 20
- Adobe Reader XI
- Adobe Shockware Player 12.1
- Java 6 Update 45
- Java 7 Update 67
- PDF Creator 1.7.2
- Citrix Online Plug-in 12.1.4
- Microsoft MSXML 4.0 SP3
- VLC Media Player 2.0.3
- Microsoft Virtual C++ 2005-2013 Redistributable packs.
- Net iD 6.1.1
- RES Workspace Manager 2014 SR2
- Netop Remote Control 12.20

3.8.1.1 Operating system

Standard client operating system is Windows 7 SP1 x64

3.8.1.2 Browser

Standard browser Internet explorer 11

3.8.1.3 Office suite

Standard office suite is Microsoft Office 2010.

3.8.2 Hardware

The standardised client platform is based on the operating system Windows 7 SP1 x64, where approximately 20 per cent are laptops and 80 per cent are desktops, 17,000 physical clients in total.

Hardware lifecycle for PCs are four years.

Mobile devices and tablets are not in use in the clinical work today, the only service provided to these devices are email synchronisation.

3.8.3 Remote Control

Netop Remote Control 12.20

3.8.4 Software distribution

Applications are delivered to computers/users either as a thick installed application or virtualised with Microsoft App-V. Software packages are streamed from a distributed file system (DFS), where a local copy of all packages are stored on all hospitals.

Security groups in AD grants users access to applications and builds collections (machine) for distribution in SCCM.

The goal is to App-V virtualise as many applications as possible and currently approximately 80 per cent of all applications are virtualised and published as App-V applications. Microsoft SCCM distributes and installs applications that are not App-V virtualised.

3.8.5 Email client

Standard email client is MS Outlook 2010.

3.8.6 Anti-virus

Microsoft System Center Endpoint Protection.

3.9 CLIENT WORKSPACE

This Chapter describes the personalised desktop configuration granted to the users on different clients.

RES Workspace Manager handles management of the user environment and profile data. Application shortcuts, user settings and print and drive mappings are distributed to the user based on the user and client context at the time of logon or reconnect.

On desktops and virtual clients, a custom created mandatory user profile is used, which is deleted from the client when the users log off. User profile settings are being preserved using RES Workspace manager and are applied to any client the user logs on.

3.10 MEDICAL DEVICES (MD) AND PERSONAL CONNECTED HEALTH AND CARE (PCHC) TECHNOLOGY

This Chapter describes the integration with and use of ***MD*** and ***PCHC technology***.

Medical devices supporting several clinical disciplines are integrated with Doculive. MDs are of different brands and support different integration standards. The main part of the MD portfolio is poor or not integrated.

There are currently no use of PCHC technology.

3.10.1 Real–time locating systems, alarm and notification systems

Real-time location systems (RTLS) use have emerged from the traditionally patient and personnel alarm and notification system use, which had similar use in the specialist health service and in the

municipal health service. As of today, RTLS are employed with slightly different objectives within specialist health service and municipal health service.

3.10.2 Current situation – RTLS in the specialist health service

RTLS utilisation is mainly focused on personnel safety, typically involved in mental health institutions. Next nascent use is tracking of equipment.

3.11 PRINT AND OUTPUT MANAGEMENT

This Chapter describes the architecture and configuration of the enterprise print service.

Print is delivered by the Microsoft Windows Printing service in cooperation with a Follow-Me print solution manufactured by Safecom.

Windows Server 2008 R2 print servers are located at each hospital and they provide Windows 7 x 64 print drivers.

Figure 16 shows the print service accessed from client and server applications.

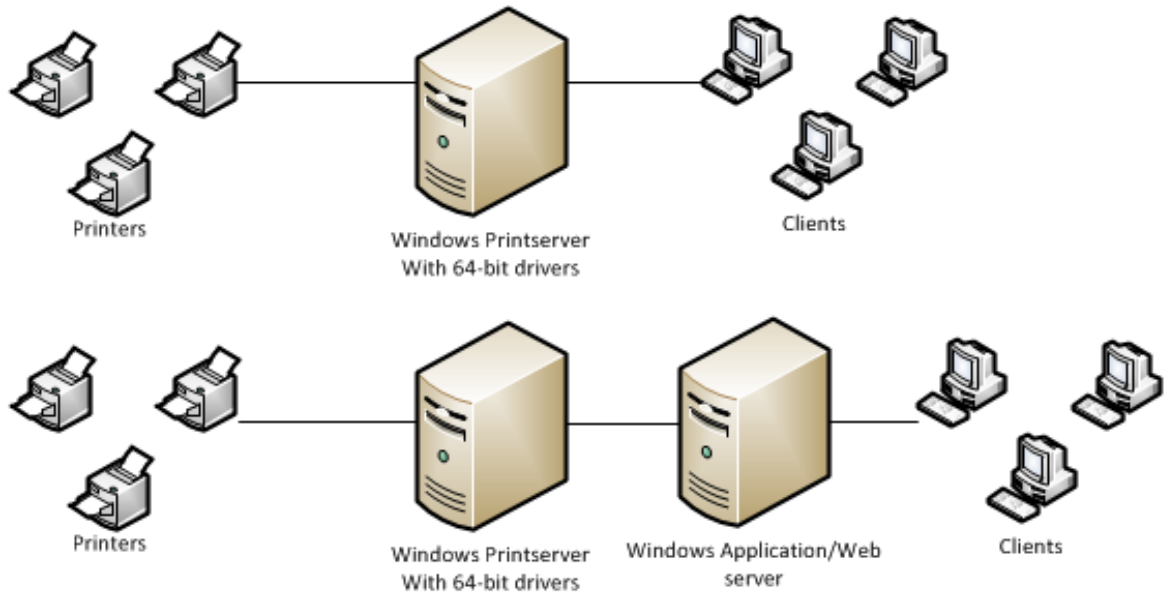


Figure 16 - Print service

Approximately 3,500-4,000 network printers are connected and about 2,000 printers are locally connected, in a variety of makes and models.

RES Workspace Manager connects the printers to the user sessions, based on the physical location of the client. Printers and clients are organised into zones, where all clients in the zone get all associated printers, connected at user logon.

3.12 IDENTITY AND ACCESS MANAGEMENT (IAM)

This Chapter describes the user and access management and the user logon functionality.

Two ***IAM*** solutions are managing the user directory. A proprietary solution developed and maintained by the specialist health service is working in parallel with the Microsoft Forefront Identity Manager (FIM).

Both solutions maintain identity data in Active Directory. The proprietary IAM solution grants users access to applications.

3.12.1 User management

The human resource (HR) system Tieto Enator PRS is managing identities of employees. Student identities are managed by the HR system operated by Norwegian University of Science and Technology (NTNU).

User identities from HR systems are populated as user objects in AD through FIM and the proprietary IAM solution.

3.12.2 User logon

Users log on to a Windows domain and authenticate using a personal certificate stored on a smartcard.

Applications authenticate users in different ways:

- Application defined username and password
- AD defined username and password
- Windows Integrated authentication provides Single Sign On

3.12.2.1 Personal user

All end users are assigned a dedicated user object in AD. Applications that are not integrated with AD are managing built in user directories.

Users granted administrative privileges are allocated a separate administrator user object.

3.12.2.2 Non personal user

Applications and system services use privileged system users defined in AD to logon to the Windows domain.

Clients of type Special log on the Windows domain with a dedicated system user at start-up.

3.13 TEST ENVIRONMENTS

This Chapter describes the test environments and the test management system.

Several test environments are established for the current ***Doculive*** EHR system to isolate testing activities from the production environment.

Dedicated test users are defined in the test environments used to test patches, new builds and new integrations.

HP ALM provides functionality for test management.

4 TECHNICAL PLATFORM MUNICIPAL HEALTH SERVICE

The scope of this Chapter is to describe the technical infrastructure for the municipal health services, except applications and systems, as they are described in *Chapter 2*.

The objective is to give a technical description of the current technical infrastructure, the operational environment supporting the current EHR systems and their closest surroundings.

This Chapter describes the major components of the technical infrastructure, including integration services.

4.1 OVERVIEW

This Chapter describes the logically interconnected internal business services within the primary health service, the integrated external organisations, the integration services and the external services.

Figure 17 shows how the municipalities in the Central Norway Health Region offer a wide portfolio of health services, such as emergency care, health clinics, nursing homes, home care services and prison health services (medium blue cloud).

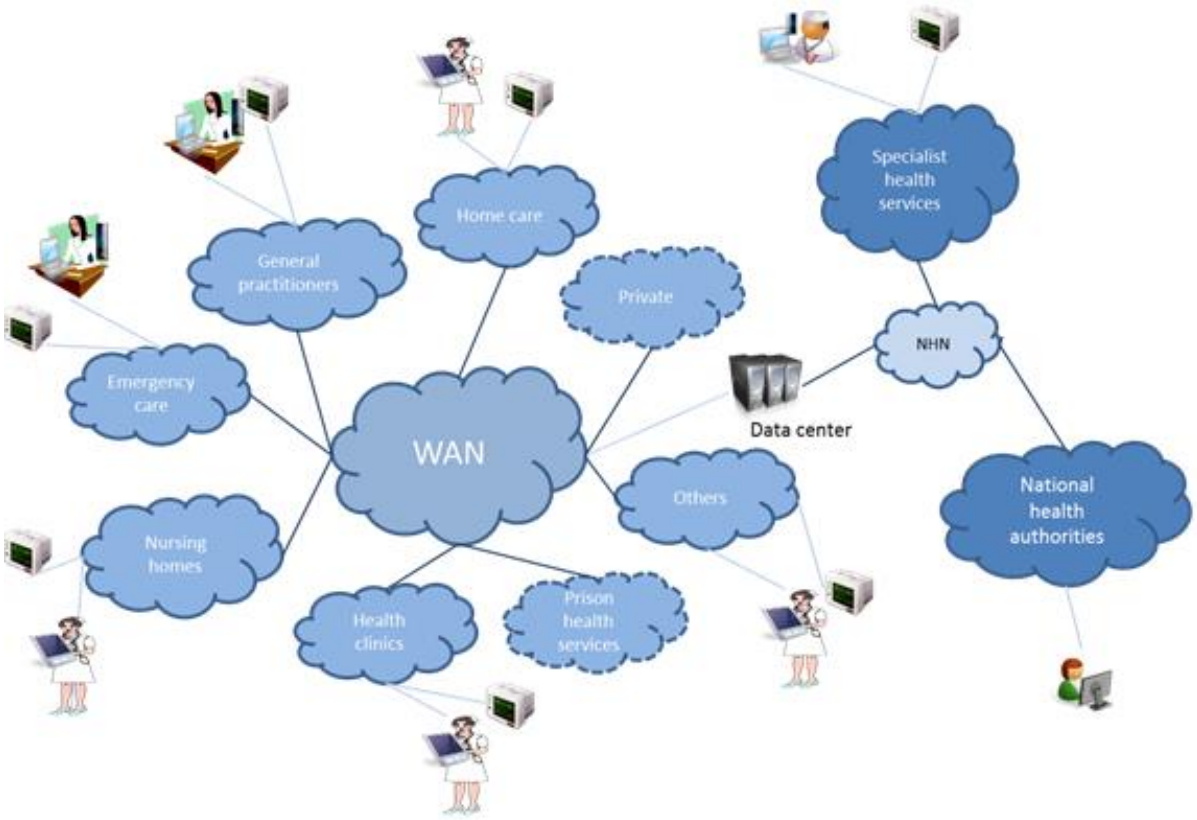


Figure 17 - Municipality health services overview

The number of services offered and their volume varies, since the number of citizens living in the different municipalities differs significantly. The categorisation of Small, Medium and Large municipalities originates from the number of citizens and the corresponding health service volume.

The Large municipalities operates high available multi-site datacentres, as several Medium municipalities are sharing high available multi-site datacentres (inter-municipal companies) or implements their own datacentres.

Small municipalities operates their own technical infrastructure based on different technical solutions.

The mandatory ***NHN*** participation connects the municipalities to the specialist and national health services by message exchange (dark blue clouds).

GPs cooperate with the municipality health services, but also integrate with the specialist health service and national health authorities by message exchange (dark blue clouds).

GPs are diversely organised. Some collaborate in a shared physical location sharing a technical infrastructure; others manage their own office and technical infrastructure.

4.2 NETWORK

This Chapter describes the different types of networks interconnecting the technical infrastructure, the network protocols used and the control mechanisms managing the traffic flow.

4.2.1 Wide Area Network (WAN)

The WAN infrastructure comprises a large number high capacity leased lines (fibre and other technologies) from different communication vendors in the market. Some link redundancy is implemented in the core part of the WAN. The City of Trondheim has implemented link redundancy throughout the core part of the WAN.

Line capacity varies from Site to Site according to the size of the organisation to interconnect.

A high capacity NHN connection provides a secure and functional electronic message exchange with the other actors in the health sector.

Cisco technology forwards and routes the IP based network traffic between Sites in the municipal health service.

4.2.2 Norwegian Health Network (NHN)

NHN, owned by the Ministry of Health and Care Services, interconnects the Norwegian health sector and supplies common application services as well as an internet connection to the connected participants. Most municipalities also maintain their own separate internet connection.

4.2.3 Local Area Network (LAN)

The LAN infrastructure comprises high capacity lines (1GB or higher), and the local network traffic is routed and forwarded by different (Cisco, HP, Other) technologies, based on a standard edge, distribution and core layered switch architecture.

4.2.4 Wireless Local Area Network (WLAN)

Wireless networks are available in some municipalities and managed clients do an automatic connect to the uniform and enterprise wireless network name (SSID). A guest wireless network is available in some municipalities for unmanaged clients.

The wireless network infrastructure comprises different technologies implemented as a centralised architecture, giving central high-available master Wireless Controllers the mandate to control the distributed slave access points (AP).

In most cases, managed PC clients connects to wireless networks by performing a successful IEEE 802.1x machine authentication.

4.2.5 Virtual Local Area Network (VLAN)

Virtual LANs partition the physical network into different logical network zones. The network traffic flows in a physical network infrastructure partitioned in different logical network zones, to support a secure and functional handling and transport of different information classes.

Figure 18 shows a typical VLAN structure used by inter-municipal companies to maintain the necessary autonomy of the participating municipalities.

Figure 19 shows a typical VLAN structure used by larger municipalities. Observe the multiplicity of client zones, which are according to the authority's guidelines and audits. The principle is to segment and minimise access to information, by allowing connection towards specific applications handling sensitive and/or enterprise internal information.

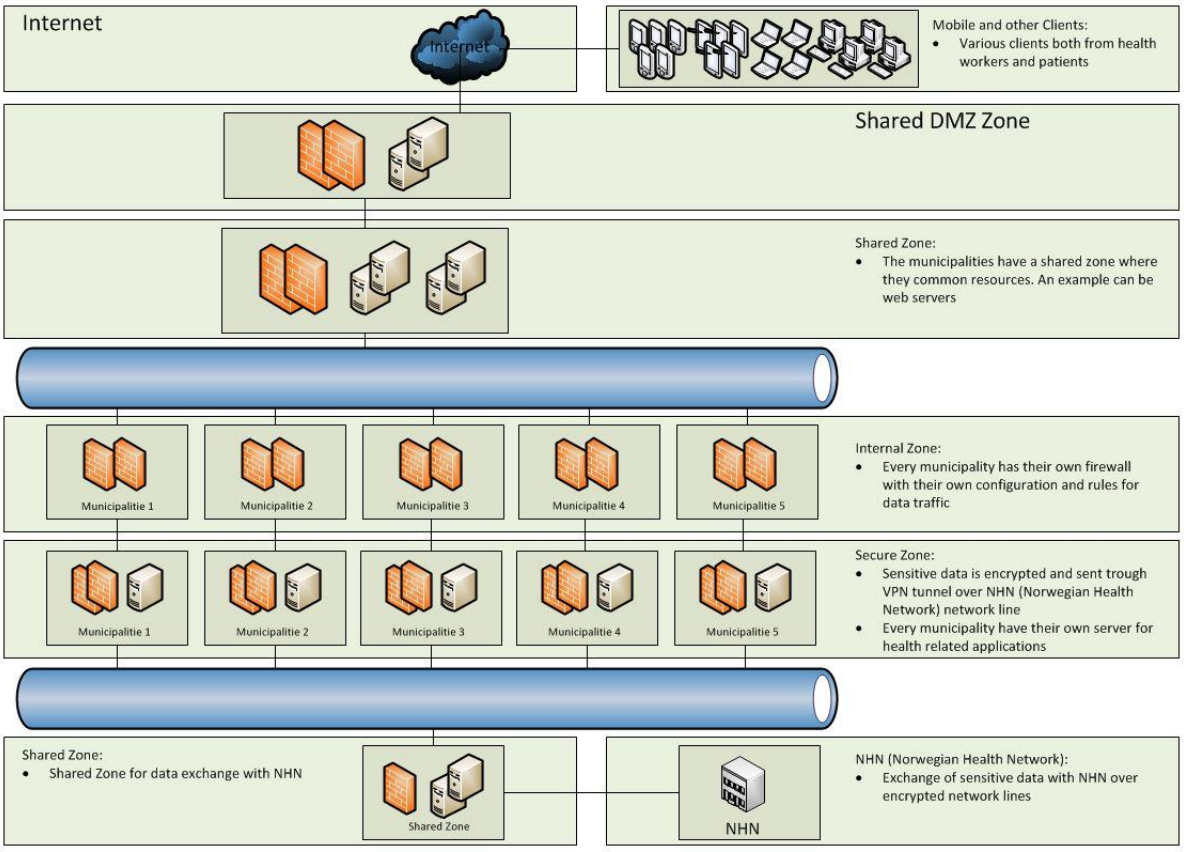


Figure 18 - Logical network zone model for inter-municipal companies serving medium and small category municipality

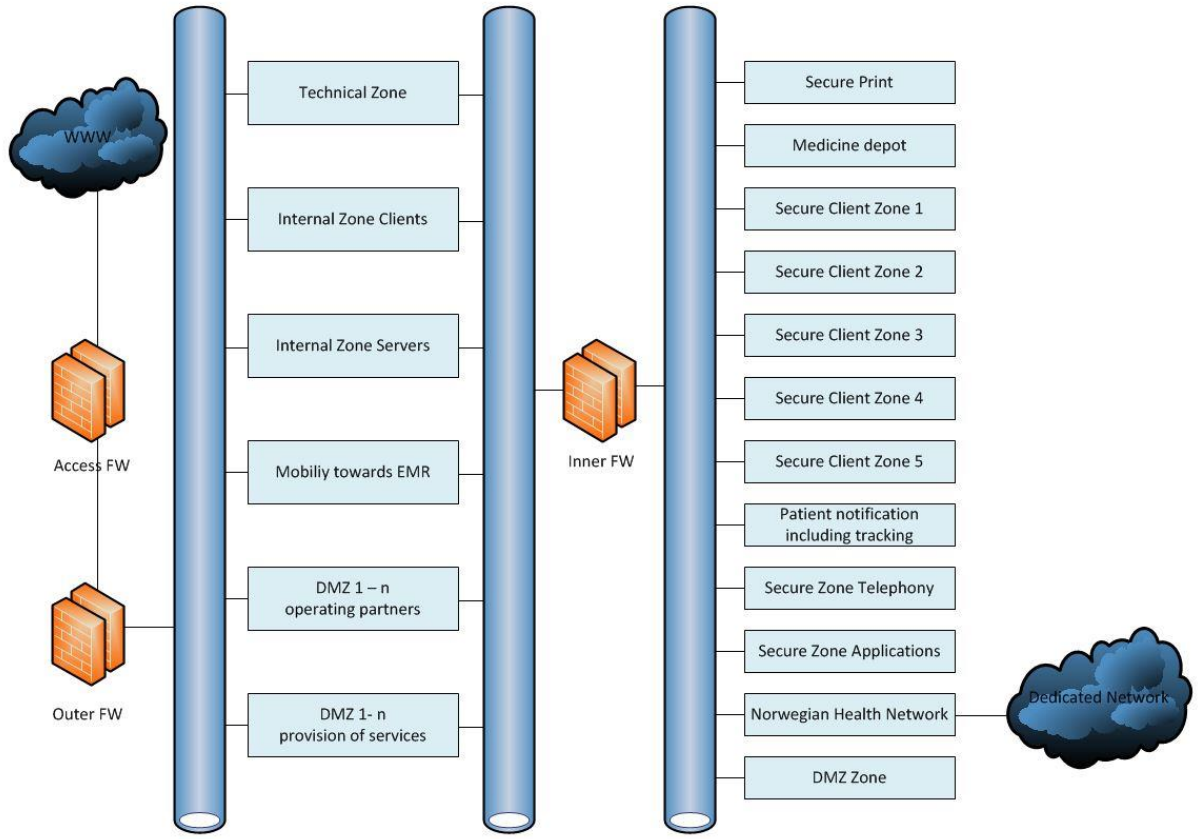


Figure 19 - Logical network zone model for large category municipality

4.2.6 Firewall

Firewalls are managing and controlling the IP network flow, ensuring an intended network flow between logical network zones. Firewall rules are managed and distributed by a central management station.

All network traffic forwarded through and blocked by the Firewall is logged.

The Firewall technologies are diverse.

4.2.7 Remote access

Remote access for employees, ***administrators*** and suppliers are diverse and based on different technologies.

4.2.8 Protocols

IP version 4 is used as the basic communication protocol.

4.3 SERVERS

This Chapter describes the infrastructure components and tools providing the production environment for applications and application services.

Small, Medium and Large municipalities may configure and version their technical infrastructure slightly different.

4.3.1 Virtual servers

A high degree of server hardware virtualisation is implemented; at least 90 per cent of the servers are virtual server instances.

All types of servers with different server roles are implemented as virtual server instances: Web servers, application servers, database servers, etc.

4.3.2 Virtualisation technology

VMWare ESXI hypervisor technology is implemented. As a deviation, some municipalities are implementing Microsoft hypervisor.

4.3.3 Physical servers

A few physical servers are used to support large database clusters and consolidated database environments with extensive workload.

4.3.4 Operating systems

The main part of the existing server infrastructure is running Microsoft Windows server OS version 2008 R2, 2012 and 2012 R2.

Just a few Oracle database and firewall systems are running Linux server operating systems.

4.3.5 Databases

Database servers can run as standalone servers and in clustered solutions.

The following configurations for database environments are implemented throughout the municipalities and the ***GPs*** in the region.

- Microsoft SQL servers in Microsoft Failover Clustered environments with several database instances in each cluster. The Microsoft SQL instances holds a consolidated production environment. This type of configuration are typically running on virtualised servers, but in a few cases on physical servers
- Virtualised non-clustered Microsoft SQL servers, running several instances. The virtualisation layer provides high availability functionality
- InterBase databases are used by some emergency systems and GPs' EHR systems
- Large municipalities are implementing Oracle ver. 10 databases and 11G RAC on top of Red hat Linux servers 5.7

4.3.6 Anti-virus

All servers are running antivirus software. Brands of antivirus software varies.

4.3.7 Backup

Backup of virtual server instances is typically performed with snapshot technologies. Some third party backup solutions are integrated with the hypervisor technologies to enhance backup functionality.

Large municipalities use IBM Tivoli Storage Manager (TSM) backup solutions.

Different methods for database backups are implemented:

- Backup is completed and stored on a file share. The backup system then pulls the finished backup to a safe and permanent storage
- The backup is performed by the database agent and stored directly into the permanent backup storage
- Primary backup is completed and stored locally on distributed StoreWize SAN. Subsequently, a synchronisation between the local and central StoreWize SAN solution takes place

4.3.8 Monitoring

The monitoring solutions used varies and are described in the subchapters below.

4.3.8.1 Network

Network Administration Visualised is a monitoring tool typically used for monitoring and configuration management. It keeps track of nodes in the network.

4.3.8.2 Server

System Center Operations Manager (SCOM) is typically used as a standard monitoring tool for servers. Hewlett Packard Business Service Management (BSM) and SiteScope are often used as a complementary monitoring tool.

4.3.8.3 Applications

Frequently used monitoring tools for application performance and availability are:

- WhatsUp Gold (former IPSWITCH), monitors network, server and application
- ZABBIX, monitors network, server and application
- The City of Trondheim makes use of SCOM and SiteScope

4.3.9 SW distribution server

Patching and updating of servers follows Microsoft best practise. Microsoft System Center Configuration Manager (SCCM) and IBM BigFix are used to automate and orchestrate server updates.

Approximately 80-90 per cent of the servers are patched automatically, the remaining servers are patched manually.

4.4 INFRASTRUCTURE SERVICES

This Chapter describes the infrastructure services used by applications to authenticate and authorise users, and distribute electronic mails

4.4.1 Active directory

The common directory service used is Microsoft Active Directory (AD).

4.4.2 Active Directory Federation Services (ADFS)

ADFS is implemented to enable access to remote web application services for local users and access to local web application services for remote users. The ADFS is implemented and in use by some municipalities.

4.4.3 PKI

Large municipalities have implemented a self-signed PKI service that issues certificates to clients, servers and users.

The local revocation information is published in AD and to a Certification Revocation List (CRL) web server.

4.4.4 Email service

The email solutions broadly used are various versions of Microsoft Exchange and Microsoft Outlook. The City of Trondheim migrates in December 2016 to G Suite for Business (GSB) G Mail.

4.5 STORAGE AREA NETWORK (SAN)

This Chapter describes general purpose mid and high-end quality data storage services.

Large municipalities use Hitachi VSP G1000 SAN and HUS-VM with real time sync between datacentres over fibre based networks. The datacentres are located on different geographically locations. The SAN solution is used for high and mid-range quality storage.

Medium and Small municipalities use different configurations for SANs. Some of the most common SAN configurations are:

- Central IBM SVC fibre channel SAN with different storage qualities
- Central IBM StoreWize fibre channel SAN with different storage qualities
- Decentralised smaller IBM StoreWize fibre channel SAN

4.6 AUTONOMOUS SUBSYSTEMS

This Chapter describes the integration system exchanging information with other parts of the health sector and the data warehouse for health management and development.

4.6.1 Data warehouse

Currently, there is limited use of data warehousing and business intelligence services in the municipalities and the ***GPs***.

4.6.2 Integrations

Municipalities and GPs integrate with external health services by message exchange, connected to the common secured ***NHN*** shared by the health sector.

Figure 20 below shows that municipal health services and GPs integrate with national health authorities (short arrows) and the specialist health service (long arrows).

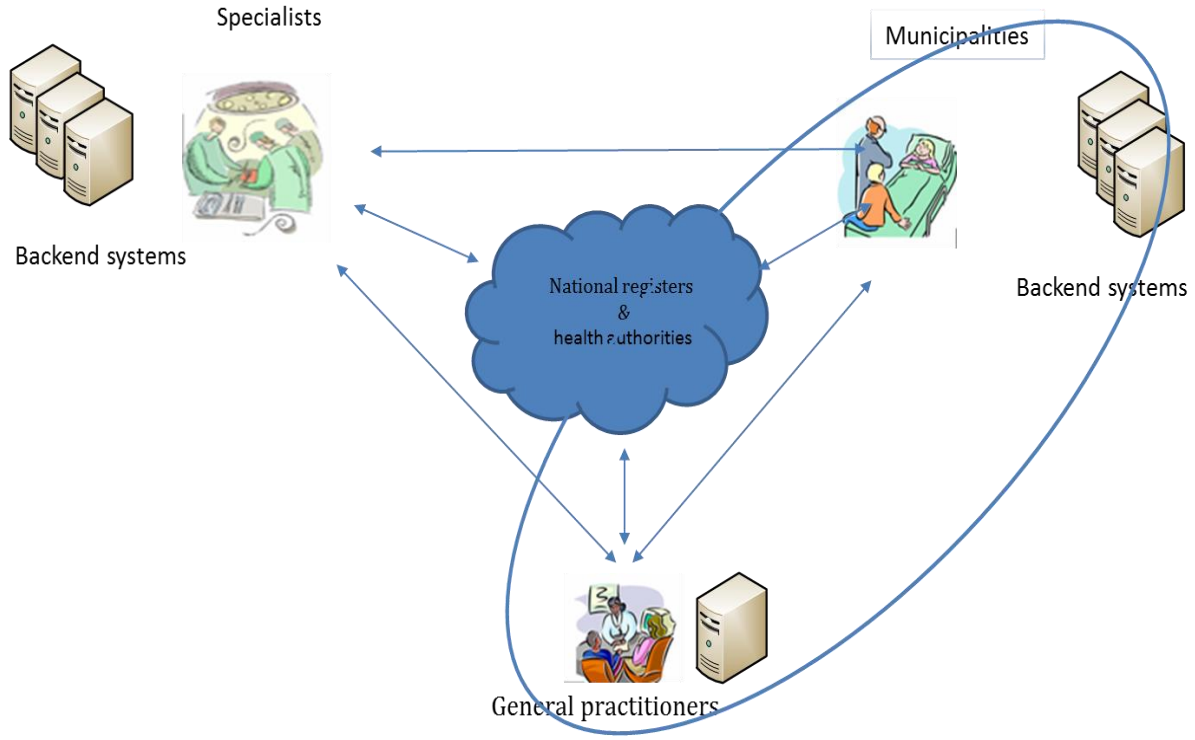


Figure 20 - Integration overview

Different EHR systems are used by different health services offered by the municipalities and GPs (Table 6). They are all bundled with EDI gateways for message exchange purposes.

Table 6 - EHR system overview

Health service	***EHR* system**
Nursing and care	CosDoc
	Gerica
	Visma Profil
GP	CGM Allmenn (Winmed)
	Infodoc Plenario
	System X
Emergency primary health care	CGM Legevakt (Winmed2)
	Infodoc Plenario
	Transmed
Public health centre	CGM Helsestasjon
	Visma Helsepro
	Infodoc Plenario

4.7 CONTINUITY

This Chapter describes the stand-by solutions to be used in an emergency incident.

The idea of the high availability solutions for the municipalities (cf. *Chapter 4.1*) are normally to produce real-time synchronised mirrored instances of the EHRs on geographically separate Sites. These instances of the redundancy then acts as the 'new' production Site during the span of an emergency incident or crisis.

There are no third instance or solution acting as 'last-resort' crises EHR-solution.

The municipality contingency management uses an external system (CIM) operated by national contingency services to manage an emergency.

4.8 CLIENTS

This Chapter describes the different client types, the hardware and basic software dependencies, and the client application configuration and distribution.

There are three different types of clients used in the municipalities:

- PC
  - Laptops and desktops
- Wyse thin client for connection to the Citrix environment
- Mobile devices like Smart Phones and PADs

The mobile smart-devices are non-personal and (re)used 24/7 by different health service personnel conducting home care services, and the number of devices in use varies with the size of the municipality. The following numbers give an idea of the prevalence of devices in concurrent use, *without* the expected increase through new PCHC services supervision.

- 60 devices in a Small municipality
- 200 devices in a Medium municipality
- 310 devices in a Large municipality

Figure 21 shows how mobile clients connect to the central server infrastructure.

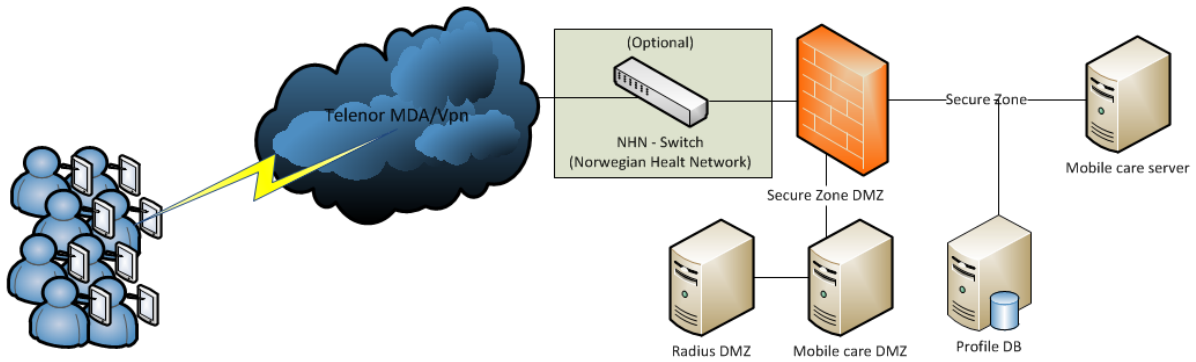


Figure 21 - Mobile clients

Access to applications managing sensitive patient information are mainly delivered through Citrix Terminal Services.

Figure 22 below shows an overview of how the PC-type clients connect to the Citrix environment.

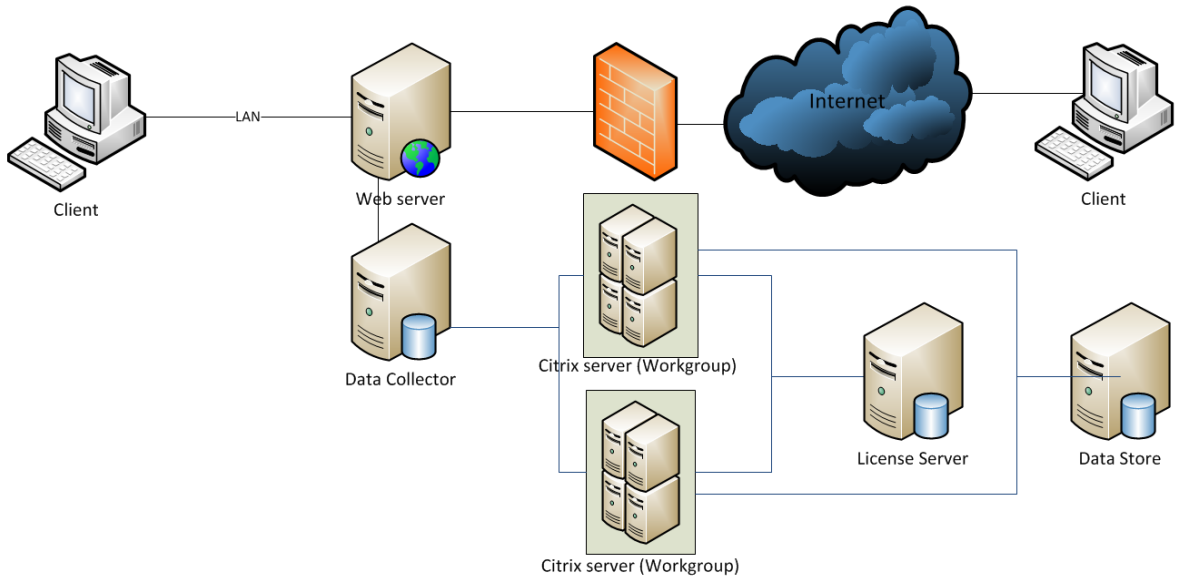


Figure 22 - PC clients, as used in both stationary and mobility context

Clients used by GPs are managed different across the municipalities. In some cases, the municipalities deliver complete solutions to the GPs and integrate the clients with the central infrastructure. In other cases, the GPs have their own independent solutions, not managed and maintained by the municipalities.

The configurations can vary both in the aspect of physical location and technology solution.

4.8.1 Hardware

The client makes and models vary across the municipalities, but can be divided into three categories:

- Intel based PC
- Apple
- Any manufacturer of smartphones and pads

4.8.2 Basic Software

4.8.2.1 Operating system

The majority of the PC clients are running Microsoft Windows 7 (mostly 64 bit), but in addition there are a number PC clients running Microsoft Windows 8.1 or Microsoft Windows 10.

The mobile devices are typically running iOS, Windows Phone 8.1 or Android.

4.8.2.2 Browser

The most common browser used on PC clients is Internet Explorer 11. Applications running on Citrix may be dependent of different versions of Internet Explorer.

The City of Trondheim uses Google Chrome as standard browser on PC clients.

For mobile devices, embedded browser on current OS version is used.

4.8.2.3 Office suite

Varied versions of Microsoft Office are installed locally on PC clients.

Applications running on Citrix may be dependent of different versions of Microsoft Office.

The City of Trondheim has started to subscribe to the G Suite for Business cloud service this year (2016).

4.8.3 Remote Control

TeamViewer and Skype for Business are primarily used for remote control of the PC clients. The City of Trondheim is using Bomgar.

4.8.4 SW distribution

Citrix Terminal Services publishes applications to users running a local installed ICA client.

Just a few applications are distributed and installed locally on the PC clients.

The GPs are installing their EHR system on PC clients.

Streaming technology (for example Microsoft App-V) is not in use for delivering applications in the current technical environment.

Some municipalities are manually configuring the mobile devices. Applications are downloaded from the associated application store and then manually installed on each device.

Large and Medium municipalities are using automated MDM solutions to configure mobile devices:

- AirWatch MDM solution for configuration and software distribution
- Citrix XenMobile 9.2 solution for configuration and software distribution

Specific for the City of Trondheim:

- Google MDM solution for configuration and software distribution concerning smart-devices used for non-sensitive information
- Citrix XenMobile solution for configuration and software distribution concerning non-personalised smart-devices used for health information and EHR solution

4.9 CLIENT WORKSPACE

This Chapter describes the personalised desktop configuration granted to the users on different clients.

Citrix XenApp Terminal Services are primarily used for health-related applications.

Citrix farms running health-related applications are located in secure zones and publishes shortcuts to the applications to the endpoint device.

Health personnel using mobile devices connect to health-related services running in secured zones.

4.10 MEDICAL DEVICES (MD) AND PERSONAL CONNECTED HEALTH AND CARE (PCHC) TECHNOLOGY

This Chapter describes the integration and use of MD and PCHC technology.

GPs EHR systems might be integrated with ***medical devices*** such as blood pressure measurements, ECG, Ultra Sound etc., but no or limited technical integrations with laboratory instruments and ***PCHC*** technology.

Medical devices are used throughout the municipalities, but with limited integrations with EHR systems.

PCHC technology is increasingly utilised in health services offered by the municipalities. Typically a response centre is monitoring the incoming messages from a variety of PCHC devices and initiate actions based on alerts or user reported medical information.

In a national context, the term PCHC technology encompasses technologies categorised as:

- confidence-building technology
- mastering own health technology
- health-technology for medical evaluation, treatment and care
- wellness technology for individual personal use but not necessary for health services

A good half of the municipalities within the Central Norway Health Region have participated in regional and national PCHC technology projects during the timespan of 2009-2015.

Typically small scale test and trial projects with 2-10 participants per project and participating municipality, within the confidence-building, mastering and health PCHC technologies.

The amount of national PCHC technology projects have increased recently, broadening the participation to 50-200 patients per municipality/project. Eight municipalities from the region contribute to these national projects.

Typical PCHC technology devices used within the proximity of the patient used in these projects are:

- Digital medication dispenser with alerts
  - when administration of medication is due
  - and if not taken
- Bed occupancy sensors and pressure mats
- Fall detectors
- Sensors or locks both for single and multiple doors and in-door geofences
- Health or medical centred devices to measure weight, blood pressure and pulse to monitor health condition

- Used for distant evaluation, treatment and care of chronical hearth disease and chronic obstructive pulmonary (COPD) disease patients

- Mobile digital personal safety alarms with audio or telephonic communication towards a response centre

- GPS personal locating or tracking system with multiple defined 'legal' geo-zones

The list above is not exhaustive.

During 2017 there is expected to be a noticeable growth (approximately 6000 devices), mainly of mobile digital safety alarms within the confidence-building PCHC technology area. Primarily to ensure two-ways voice between patient and response centre, secondly to apply and monitor a variety of alarm sensors.

Large municipalities plan to offer PCHC technology as part of their sanctioned health services during 2018-2020.

Figure 23 below shows the current implemented PCHC technology solutions in the larger municipalities and the their limited integration with the EHR systems.

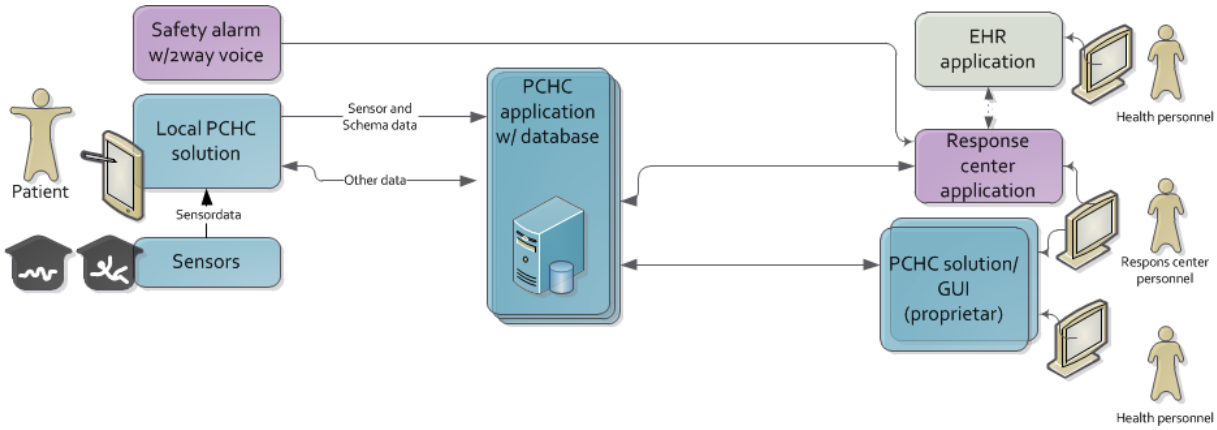


Figure 23 - Current limited integration with EHR systems

4.10.1 Real–time locating systems, alarm and notification systems

Use of real-time location systems (RTLS) have emerged from the traditional patient and personnel alarm and notification system use, which had similar use in specialist and municipality health service.

As of today, RTLS are employed with slightly different objectives within specialist health service and municipal health service.

4.10.1.1 Current status – RTLS in municipal health services

RTLS systems are typically used within nursing homes and assisted living or residential care homes. The utilisation is to locate patients and nursing personnel, to control door locks according to authorisation, to maintain area geofencing and to obtain and manage aberrant location alarms within patient rooms.

Prevalence within municipalities may vary.

The City of Trondheim has implemented RTLS tracking technology in 14 of its 32 larger nursing homes and some assisted living or residential care homes. Future migration from traditional

alarm and notifications systems to RTLS occurs at a rate of approximately four nursing homes per year by this municipality.

Examples of systems deployed are Elpas from TE Connectivity (former Tyco Electronics) and Televagt from Tunstall.

4.11 PRINT AND OUTPUT MANAGEMENT

This Chapter describes the architecture and configuration of the print service.

Standard Windows print functions are used for printing from client applications.

Follow-me print solutions are available to users based on roles and needs. The Follow-me print solutions are based on the Windows print service.

The City of Trondheim uses in addition some other printing solutions:

- Google cloud print from some client applications
- Everyone Print for printing from mobile smart-devices
  - Everyone Print solution function through a Follow-me solution.

4.12 IDENTITY AND ACCESS MANAGEMENT

This Chapter describes the shared user directory, the user management and the user logon functionality.

GPs are using X.509 v3 qualified certificates on smartcards to authenticate to the EHR systems. Large municipalities are using X.509 v3 non-qualified certificates on smartcards to logon to both security domains and normal domains.

The most common authentication method used throughout the municipalities is username and passwords combinations.

4.12.1 User management

All identities are synchronised from identity sources (typically HR systems) and populated to Active Directory as separate user objects.

Authorisations are granted to users based on group membership in Active Directory.

4.12.2 User Logon

No single sign-on functionality is provided for restricted health service applications.

4.12.2.1 Personal user

Users accessing health service applications are defined in separate user objects.

4.12.2.2 Non personal user

Users of type system or service users are used by applications and databases at start-up time.