DIGISTAT® Mobile
User Manual

DIGISTAT® V5.1

DIG MOB IU 0007 ENG V02 - 17 October 2018

ASCOM UMS s.r.l. Unipersonale

Via Amilcare Ponchielli 29, 50018, Scandicci (FI), Italy

Tel. (+39) 055 0512161 – Fax (+39) 055 829030

www.ascom.com

DIGISTAT® version 5.1

SOFTWARE LICENSE

Your Licence Agreement – provided with the product - specifies the permitted and prohibited uses of the product.

LICENSES AND REGISTERED TRADEMARKS

DIGISTAT® is produced by ASCOM UMS s.r.l
http://www.ascom.com
DIGISTAT® is a Trademark of ASCOM UMS s.r.l
Information is accurate at the time of release.
All other trademarks are the property of their respective owners.

DIGISTAT® product is CE marked according to 93/42/CEE directive (“Medical devices”) amended by the 2007/47/EC directive.

ASCOM UMS is certified according to UNI EN ISO 9001:2015 and UNI CEI EN ISO 13485:2012 standards for “*Product and specification development, manufacturing management, marketing, sales, production, installation and servicing of information, communication and workflow software solutions for healthcare including integration with medical devices and patient related information systems*”.

Contents

1. Using the manual 8

1.1 Aims 8

1.2 Characters used and terminology 9

1.3 Symbols 10

2. Introduction to DIGISTAT® 11

2.1 Modular Architecture 11

2.2 Intended use 11

2.2.1 Safety Advisories 13

2.3 "Off-label" use of the Product 14

2.4 CE mark and regulation conformity 14

2.5 Manufacturer's responsibility 16

2.6 Product traceability 16

2.7 Post-market surveillance 16

2.8 Product life 17

3. Software/Hardware specifications 18

3.1 Central & Bedside 18

3.1.1 Hardware 18

3.1.2 Operating System 19

3.2 Server 19

3.2.1 Hardware 19

3.2.2 Operating System 19

3.2.3 System Software 19

3.3 DIGISTAT® "Mobile" 19

3.4 DIGISTAT® “Web” 20

3.5 General warnings 21

3.6 Firewall and Antivirus 22

3.6.1 Further recommended precautions for cyber-protection 22

3.7 Local network features 23

3.7.1 DIGISTAT® system impact on the healthcare organization network 24

4. Before starting 25

4.1 Installation and maintenance warnings 25

4.1.1 Patient Area 26

4.2 Cleaning 27

4.3 General precautions and warnings 27

4.3.1 Electrical safety 28

4.3.2 Electromagnetic compatibility 28

4.3.3 Devices eligibility 28

4.4 Privacy Policy 29

4.4.1 User credentials features and use 32

4.4.2 System administrators 33

4.4.3 System logs 34

4.5 Backup policy 34

4.6 Out of order procedure 34

4.6.1 Reconfiguration/substitution of network equipment 36

4.7 Preventive maintenance 36

4.8 Compatible devices 39

4.9 System unavailability 39

5. DIGISTAT® Mobile 41

5.1 Information for the user 41

5.2 Start-up 43

5.2.1 Authorizations for proper functioning 43

5.2.2 ASCOM MYCO (w/ Unite) Start-Up 47

5.2.3 Android device start-up 48

5.2.4 Updates installation (APK files) 51

5.3 Lateral Menu 51

5.4 Login 53

5.5 Upper notification bar 55

5.6 General System Notifications 55

5.6.1 Sound Check procedure 57

5.6.2 Check System procedure 59

5.7 Patient’s search functionalities 62

5.7.1 Textual search 63

5.7.2 Barcode Scan search 66

5.7.3 NFC Reader search 66

5.7.4 Single Patient Selection 68

5.8 Patients Assignment Functionality 70

5.9 Patient selection/assignment, modules and domain 73

6. DIGISTAT® Smart Central Mobile 74

6.1 Introduction 74

6.2 Application start-up 74

6.3 “Central” screen 75

6.4 Medical devices list 78

6.4.1 Heading 78

6.4.2 Devices list 79

6.5 Alarms history 81

7. DIGISTAT® “Vitals” 82

7.1 Introduction 82

7.2 Application start-up 82

7.3 Patients list 83

7.3.1 Patient list heading 84

7.3.2 List of beds 84

7.4 Datasets list 85

7.4.1 How to record a new set of data 87

7.4.2 Inserted values summary 89

7.4.3 How to edit an existing set of data 90

7.4.4 Pictures and audio acquisition 91

7.4.5 How to use OCR functionality 96

7.5 Enabling and configuring the existing datasets 102

8. DIGISTAT® “Voice Notes” 105

8.1 Introduction 105

8.2 Application start-up 105

8.2.1 Users access 106

8.2.2 Notifications 107

8.3 Patients list 108

8.3.1 Patient list heading 108

8.3.2 List of beds 109

8.4 Voice messages list 109

8.4.1 Listening to voice messages 111

8.4.2 Delete a voice message 112

8.4.3 Record a voice message 113

9. DIGISTAT® “Identity” 116

9.1 Introduction 116

9.2 Application Start-Up 116

9.2.1 Main view 117

9.2.2 List of unassigned device 117

9.2.3 List of assigned device 118

9.3 Set association workflow 119

9.3.1 Start of the process 119

9.3.2 Identification of the patient 119

9.3.3 Confirmation of patient identification 121

9.3.4 Device identification 123

9.3.5 Confirmation of device identification 123

9.4 Unset association workflow 124

9.4.1 Start of the process 124

9.4.2 Device identification 124

9.4.3 Confirmation of device identification 125

10. Manufacturer Contacts 126

11. Residual risks 127

1. Using the manual

1.1 Aims

The effort which has gone into creating this manual aims to offer all the necessary information to guarantee a safe and correct use of the DIGISTAT® system and to allow the manufacturer identification. Furthermore, this document aims to describe every part of the system, it also intends to offer a reference guide to the user who wants to know how to perform a specific operation and a guide for the correct use of the system so that improper and potentially hazardous uses can be avoided.

The use of DIGISTAT® requires a basic knowledge of information systems concepts and procedures. The comprehension of this manual requires the same knowledge.

Always remember that DIGISTAT® systems are highly configurable, in order to satisfy the requirements of every user. This flexibility makes it difficult to provide a description of all the system's possibilities. Hence the manual describes "probable", or "standard" configuration, in an effort to explain the fundamental parts of the system, and their purposes. Consequently, the user may come across descriptions of screens and functions that differ from their actual configuration.

To be more precise, the differences may concern

- The appearance of the screen (a screen may appear different from that shown here).
- The functions (certain operations may or may not be enabled).
- The flow of use (certain procedures can be performed following a different sequence of screens and actions).

Specific warnings are provided when the configuration options allow multiple possibilities.

Should more details regarding a specific configuration be required, please contact your system administrator or the ASCOM technical support service.

1.2 Characters used and terminology

The use of DIGISTAT® systems requires a basic knowledge of the most common IT terms and concepts. In the same way, understanding of this manual is subject to such knowledge.

Remember that the use of DIGISTAT® systems must only be granted to professionally qualified and properly trained personnel.

When consulting the online version as opposed to the paper version, cross-references in the document work like hypertext links. This means that every time you come across the reference to a picture (e.g. “Fig 11”) or to a paragraph / section (e.g. “paragraph 2.3.1”), you can click the reference to directly go to that particular figure or that particular paragraph / section.

Every time a reference is made to a button, this is written “**Bold**”. For example, in expressions like:

➢ Click the “**Update**” button,

“**Update**” is a button featured on the screen being described. Where possible, it is clearly indicated in a figure (with cross references as “See Fig 13 **A**”.

The character ➢ is used to indicate an action which the user must perform to be able to carry out a specific operation.

The character ● is used to indicate the different items of a list.

1.3 Symbols

The following symbols are used in this manual.

i	**Useful information** This symbol appears alongside additional information concerning the characteristics and use of DIGISTAT® Systems. This may be explanatory examples, alternative procedures or any "extra" information considered useful to a better understanding of the product.

!	**Caution!** The symbol is used to highlight information aimed at preventing improper use of the software or to draw attention to critical procedures which might cause risks. Consequently, it is necessary to pay extreme attention every time the symbol appears.

The following symbols are used in the DIGISTAT® information box (paragraph 5.3):

🏭	The manufacturer's name and address
📖ℹ	Attention, consult accompanying documents

2. Introduction to DIGISTAT®

The DIGISTAT® clinical modules suite is an advanced patient data management software system that is designed specifically for use by clinicians, nurses and administrators.

The software package consist of a set of modules that can either work alone or be fully integrated to provide a complete patient data management solution.

From the Intensive Care Unit to the Ward, from the Operating Room to the Administrative Department, DIGISTAT® systems can be used in a wide range of environments.

DIGISTAT®'s modular architecture and extensive customization Configuration capabilities allows the patient data management system to be tailored to organizational needs and adaptable to meet new demands when required.

DIGISTAT® system can only be accessed by entering username and password. Every user is defined by a detailed profile and can access only the allowed areas. An audit trail of every login performed is automatically generated by the system.

2.1 Patient Population

The product is a software application and is not in contact with the patient.
Intended patient population is defined as follows:
* Patient weight between 0.1kg and 250kg
* Patient height between 15cm and 250cm
* No other limitations

2.2 Modular Architecture

“Modular Architecture” means that different applications (or modules) can be implemented within the same software environment (DIGISTAT® in the present case) that is characterized by a consistent user interface, same overall goals and terms of use.

Modules can be added at different times, and in a way that is agreed with the user. The resultant software suite fits the specific user needs and can change in time, according to the possible changes in the user needs.

2.3 Intended use

The DIGISTAT Software (hereafter “Product”) acquires records, organizes, transmits and displays patient information and patient related data, including data and events from connected clinical devices and systems as well as information entered manually, in order to support caregivers in diagnosis and treatment of patients as well as to establish electronic patient records.

- The Product produces configurable electronic patient records based on acquired data and information, as well as on manual and automated documentation of the clinical unit's activity.
- The Product provides automated, secondary visual and audible announcing and displaying of acquired data, events, current status and operating conditions of connected clinical devices and systems on designated display device(s). The Product can also be configured to forward data and information about events, statuses and operating conditions to the ASCOM messaging system.
- The Product supports the improvement of nursing workflows related to the management of alarms from the connected clinical devices and systems.
- The Product supports the documentation of the prescribed therapy, its preparation and its delivery.
- The Product supports the recording, validation and display of vital signs charting based on the acquired data and information.
- The Product provides configurable reports, charts and statistics based on recorded data for use by healthcare professionals to analyze the unit's efficiency, productivity, capacity and resource utilization, and the quality of care.

The Product **does not** replace or replicate the original display of data and alarms of the connected devices and systems and **does not** control, monitor or alter the behavior of these connected devices and systems, or their associated alarms.

The Product **is not** intended to be used for direct diagnosis or monitoring of vital physiological parameters.

The Product is intended for use by trained healthcare professionals within a hospital/clinical environment and relies on proper use and operation of the IT and communication infrastructure in place at the healthcare facility, the display devices used and the connected clinical devices and systems.

Additionally, the Product provides specific functions and interfaces intended to be used by non-professional users in remote locations for non-clinical purposes for display of information, reports, charts and statistics, without the ability to add, change or delete any information or data.

The Product is a stand-alone software that is installed on servers and computers, which must comply with the technical hardware and software specifications provided with the Product.

2.3.1 Safety Advisories

The Product, even if designed to provide very high accuracy, cannot guarantee the complete and correct communication of the acquired data, nor can it substitute the direct verification of the same by the User.

The User shall base therapeutic or diagnostic decisions and interventions solely on the direct examination of the original source of information. The user has sole responsibility to check that the information displayed by the Product is correct and to make appropriate use of it**.**

In any case, the Product must be used in compliance with the safety procedures reported in the user documentation accompanying the Product.

Only printouts that are signed with digital or ink signature by authorized medical professionals shall be considered valid clinical records. In signing the aforementioned printouts, the User certifies they have checked the correctness and completeness of the data present in the document.

Only these signed documents are a valid source of information for diagnostic or therapeutic processes and/or procedures.

The Product can be used in the proximity of the patient and to the connected clinical devices in order to speed up the data entry, to reduce the probability of errors and to allow the User to verify the correctness of the data through the immediate comparison with the actual data and activities.

When entering patient related data the User shall verify that the patient identity, hospital department/care unit and bed information displayed in the Product are correct. This verification is of utmost importance in cases of critical interventions, for instance, drug administration.

The Responsible Organization must establish and implement appropriate procedures to ensure that potential errors occurring in the Product and/or in the use of the Product are promptly detected and corrected and do not constitute a risk to the patient and the User. These procedures depend on the configuration of the Product and the method of use preferred by the organization.

The Product may provide, depending on the configuration, access to information on drugs. The Responsible Organization shall, initially and periodically, verify that this information is current and updated.

The Product must not be used in place of the direct monitoring of the alarms generated by the medical devices. This limitation is due, among the other reasons, to the specifications and limitations of the communication protocols of the medical devices.

Where devices used with the Product are located in the patient area or are connected to equipment present in the patient area then the Responsible Organization shall ensure that the whole combination complies with the international standard IEC 60601-1 and any additional requirement(s) established by the local authorities.

Use of the Product must be granted, by means of specific configuration of the passwords and active surveillance, only to User who are:

- trained according to Product indications by personnel authorized by the manufacturer or distributors and
- in possession of the professional qualifications to correctly interpret the information supplied and to implement the appropriate safety procedures.

The Product is a stand-alone software that can run on standard computers and/or standard mobile devices connected to the hospital local network. The computers, devices and the local network shall be adequately protected against cyber-attacks.

The Product shall be installed only on computers and devices fulfilling the minimum hardware requirements and on supported operating systems.

2.4 “Off-label” use of the Product

Every use of the Product outside what explicitly stated in the “Intended use” (usually referred to as “off-label” use) is under the full discretion and responsibility of the user and of the Responsible Organization.

The manufacturer does not guarantee in any form the Product safety and suitability for any purpose where the Product is used outside the stated “Intended use”.

! The Product **is not** a primary remote alarm system.

2.5 CE mark and regulation conformity

ASCOM UMS DIGISTAT® product is CE marked according to 93/42/EEC directive (“Medical devices”), amended by the directive 2007/47/EC, and is therefore compliant with the EU basic safety standards there specified (received in Italy with Legislative Decree n. 37/2010 and subsequent variants and integrations).

ASCOM UMS declines all responsibility for the consequences on the safety and efficiency of the product determined by technical repairs or maintenance not performed by its own Technical Service personnel or by ASCOM UMS-authorized technicians.

The attention of the user and the legal representative of the Healthcare Organization where the device is used is drawn to their responsibilities, in view of the local legislation in force on the matter of occupational safety and health (e.g. in Italy Dlgs. no. 81/2008) and any additional local site safety.

The ASCOM UMS Service is able to offer customers the support needed to maintain the long-term safety and efficiency of the devices supplied, guaranteeing the skill, instrumental equipment and spare parts required to guarantee full compliance of the devices with the original construction specifications over time.

2.6 Manufacturer’s responsibility

ASCOM UMS is responsible for the product’s safety, reliability and performance only if:

- Installation and configuration were performed by personnel trained and authorized by Ascom UMS;
- Use and maintenance comply with the instructions provided in the Product documentation (including this User Manual);
- Configurations, changes and maintenance are only performed by personnel formed and authorized by ASCOM UMS ;
- The Product’s usage environment complies with applicable safety instructions and applicable regulations;
- The environment in which the Product is used (including computers, equipment, electrical connections, etc.) complies with applicable local regulations.

! Should the Product be part of a “medical electrical system” through electrical and functional connection with medical devices, the healthcare organization is in charge of the required electrical safety verification and acceptance tests, even where ASCOM UMS performed in whole or in part the necessary connections.

2.7 Product traceability

In order to ensure device tracking and ongoing safety and efficiency checks on site, in compliance with ISO 9001 and EN 13485 quality standards and European law on medical devices 93/42/EEC, amended by the directive 2007/47/EC, the former Product owner is recommended to inform ASCOM UMS/Distributor about any ownership transfer by giving written notice stating the product, former owner and new owner identification data.

Product data can be found in the product labeling (either paper label provided at installation time or “About box” displayed within the product – see paragraph 5.3).
In case of doubts/questions about product labeling and/or product identification please contact ASCOM UMS/Distributor technical assistance (for contacts see section 8).

2.8 Post-market surveillance

The CE marked device is subject to a post-market surveillance. ASCOM UMS, its distributors and dealers must provide, for each marked copy, information concerning actual and potential risks, either for the patient or the User, during the Product’s life cycle.

In case of deterioration of the Product characteristics, poor performance or inadequate user instructions that have been or could be a hazard to either the patient or User' health or to environmental safety, the User must immediately give notice to either ASCOM UMS, one of its branches or nearest authorized dealer.

The product details can be found on its labeling.

On reception of a user feedback ASCOM UMS will immediately start the review and verification process and, when required, solve the reported nonconformity.

2.9 Product life

The life time of the product does not depend on wearing or other factors that could compromise safety. It is influenced by the obsolescence of the hardware (computer and server) and is therefore assessed as 5 years since the release date of the product-specific version. During this period ASCOM UMS is committed to keeping technical documentation and provide technical support.

3. Software/Hardware specifications

! DIGISTAT® must only be installed by trained authorized personnel. This includes Ascom UMS/Distributors staff and any other person specifically trained and explicitly authorized by Ascom UMS/Distributor. Without an explicit, direct authorization from Ascom UMS/Distributor, the healthcare organization staff are not authorized to perform installation procedures and/or to modify DIGISTAT® configuration.

! DIGISTAT® must only be used by trained personnel. DIGISTAT® cannot be used without having a proper training, performed by Ascom UMS/Distributors staff.

The information provided in this chapter covers the manufacturer's obligations identified by the IEC 80001-1:2010 standard (Application of risk management for IT-networks incorporating medical devices).

According to the IEC 60601-1 standard, in case where an electrical equipment is positioned close to the bed, the use of "Medical grade" devices is required. In these situations medical grade PANEL PCs are usually used. If explicitly requested, ASCOM UMS is able to provide information on appropriate devices.

! In order to display the electronic version of the instructions for use (PDF files), Adobe Reader or any other PDF reader shall be installed

3.1 Central & Bedside

3.1.1 Hardware

Minimum hardware requirements:

- Intel® I3 processor (or faster)
- Memory: 4 GB RAM
- Hard Disk: at least 60 GB of available space
- Monitor: 1024 x 768 or higher (1920 x 1080 suggested)
- Mouse or other compatible device
- Ethernet interface 100 Mb/s (or higher)
- CD/DVD Drive or possibility to copy the installation files

3.1.2 Operating System

- Microsoft Corporation Windows 7 SP1 x86/x64 Professional
- Microsoft Corporation Windows 8.1 x86/x64 Professional
- Microsoft Corporation Windows 10

3.2 Server

3.2.1 Hardware

Minimum hardware requirements:

- Intel® I5 processor (or faster)
- Memory: 4 GB RAM (8 GB recommended)
- Hard Disk: at least 120 GB of available space
- Ethernet interface 100 Mb/s (or higher). Suggested 1 Gb/s.
- CD/DVD Drive or possibility to copy the installation files

3.2.2 Operating System

- Microsoft Corporation Windows Server 2012 R2
- Microsoft Corporation Windows Server 2016

3.2.3 System Software

- Microsoft SQL Server 2008R2
- Microsoft SQL Server 2012
- Microsoft SQL Server 2014
- Microsoft SQL Server 2016
- Microsoft SQL Server 2017
- Microsoft Framework.NET 4.5

3.3 DIGISTAT® “Mobile”

DIGISTAT® Mobile has been verified on the ASCOM Myco SH1 Wi-Fi and Cellular Smartphone device, with Android version 4.4.2 (Myco 1) and 5.1 (Myco 2). The application is therefore compatible with Myco 1 and Myco 2. The application is designed to be compatible with other Android devices with a minimum screen size of 3.5’’, and compatibility with a specific device must be verified before clinical use.

The OCR functionality is not supported on Myco1 devices and in general on devices with Android version 4.4.2 and lower; it is supported on the Myco2 devices and in general on Myco devices with firmware version 10.1 and higher, or in general on Android devices with version 5.1 and higher.

Please contact ASCOM UMS for the full list of devices that support Digistat® Mobile.

3.4 DIGISTAT® "Web"

The following browsers are supported for use with DIGISTAT® web applications:

- Chrome 63
- Firefox 56
- Edge 41
- Internet Explorer 11

❗ Only supported Web Browsers shall be used for Digistat Web.

❗ A Digistat Web workstation shall always have the Web Browser in foreground. Besides, the Web Browser shall never be used for anything else but Digistat Web (which also implies that the Digistat Web homepage shall be the default homepage of the Web Browser).

❗ The Browser's Display Scaling shall always be set to 100%.

❗ When the local network is at least partially based on WiFi connections, given the intermittent nature of WiFi connections, disconnects could occur which activate the Disconnected Mode (grey carpet covering Digistat Web) and thus the system may not be available. The Healthcare Organization must work to ensure optimal WiFi coverage and instruct the staff on how to handle these temporary system outages.

3.5 General warnings

To correctly use DIGISTAT®, the Microsoft Windows Display Scaling must be set to 100%. Different settings may prevent the product from starting or cause malfunctions in the way DIGISTAT® system is visually displayed. Please refer to the Microsoft Windows documentation for instructions on the Display Scaling settings.

The minimum vertical resolution of 768 is supported only if DIGISTAT® system is configured to run in full-screen mode or if the Windows tray bar is in Auto-hide mode.

The computers and the other connected devices must be suitable for the environment in which they are used and must, therefore, comply with the relevant regulations.

It is mandatory to follow the manufacturer instructions for storage, transport, installation, maintenance and waste of third parties hardware. These procedures must be performed only by qualified and authorized personnel.

The use the Product together with any software other than those specified in this document may compromise the safety, effectiveness and design controls of the Product. Such use may result in an increased risk to users and patients. It is mandatory to consult an authorized ASCOM UMS or Distributor technician before using together with the Product any software other than those specified in this document.

If the hardware on which the Product runs is a stand-alone computer, the user shall not install any other software (utilities or applications programs) on the computer. It is suggested to apply a permission policy that prevents users from performing procedures such as the installation of new software.

! The Responsible Organization shall implement for the DIGISTAT® workstations a date/time synchronization mechanism to a reference source.

! It is recommended to disable the access to Internet on the client workstations and the handheld devices on which the Product is used. Alternatively the healthcare organization shall implement the necessary security measures in order to guarantee adequate protection from cyber-attacks and installation of unauthorized applications.

3.6 Firewall and Antivirus

To protect the DIGISTAT® system from possible cyber-attacks, it is necessary that:

- The Windows© Firewall is active both on the client PCs and the server;
- Antivirus/antimalware software is installed and regularly updated both on the client PCs and the server.

The Healthcare Organization shall ensure that these two protections are activated. ASCOM UMS tested the Product with F-SECURE Antivirus but, considering the strategies and policies already existing in the healthcare Organization, the actual choice of the antivirus is left to the Responsible Organization. ASCOM UMS cannot ensure that the DIGISTAT® system is compatible with any antivirus or antivirus configuration.

! Some incompatibilities have been reported between parts of DIGISTAT® and Kaspersky antivirus. The solution to these incompatibilities required the definition of specific rules in the antivirus itself.

! It is suggested to only keep open the TCP and UDP ports actually needed. These may change according to the system configuration. Please refer to the ASCOM UMS technical assistance for more information.

3.6.1 Further recommended precautions for cyber-protection

In order to further protect the DIGISTAT® system from possible cyber-attacks, it is highly recommended to:

- plan and implement the “Hardening” of the IT infrastructure including the IT platform that represent the runtime environment for the Product,

- implement an Intrusion Detection and Prevention System (IDPS),
- perform a Penetration Test and, if any weakness is detected, perform all the required actions to mitigate the risk of cyber-intrusion,
- dismiss the devices when they are no longer updatable,
- plan and perform a periodic verification of the integrity of files and configurations,
- Implement a DMZ (demilitarized zone) solution for web servers that need to be exposed on the internet.

3.7 Local network features

This section lists the features of the local network on which DIGISTAT® system is installed in order to guarantee the system's full functionality.

- DIGISTAT® system uses a TCP/IP traffic protocol.
- The LAN must not be congested and/or full loaded.
- DIGISTAT® system requires at least a 100 Megabit LAN available to the client workstation. 1 Gigabit Ethernet backbone~~s~~ would be worthwhile.
- There must not be filters in the TCP/IP traffic between workstations, server and secondary devices.
- If the devices (server, workstations and secondary devices) are connected to different subnets there must be routing in these subnets.
- It is recommended to adopt redundancy strategies to ensure network service availability in case of malfunction.
- It is recommended to schedule, together with ASCOM/Distributors, the maintenance calendar in order to let ASCOM or the authorized Distributor efficiently support the healthcare organization in managing the possible disservices caused by maintenance activities.

! If the network does not match the requested features, DIGISTAT® system performance gradually deteriorates until timeout errors occur. The system may finally switch to "Recovery" mode.

! In case a WiFi network is in use, given the possible intermittency of the WiFi connection, network disconnections are possible, that cause the activation of the "Recovery Mode" and the consequent system unavailability. The Responsible Organization shall ensure an optimal network coverage and stability, and train the personnel in the management of these temporary disconnections.

! In order to encrypt the data transmitted over wireless networks it is recommended to adopt the highest security protocol available; in any case no less than WPA2.

3.7.1 DIGISTAT® system impact on the healthcare organization network

DIGISTAT® system impacts the local network of the healthcare organization. This section provides information on the traffic generated by the DIGISTAT® system on the network in order to make it possible for the structure to evaluate and analyze the risks related to the introduction of the DIGISTAT® system.

The bandwidth used by a DIGISTAT® system depends on many different factors. The most important are:

- Number of workstations,
- Number of workstations configured as central stations,
- Number and type of devices dedicated to data acquisition
- Interfaces with external systems,
- DIGISTAT® system configuration and mode of use.

DIGISTAT® bandwidth occupation depends mainly on data acquisition from medical devices. In a configuration with acquisition on 100 beds where every bed collects data from 1 ventilator, 1 patient monitor and 3 infusion pumps, and with 10 DIGISTAT® workstations covering 10 beds each, the following bandwidth occupation values can be indicatively predicted:

Average: 0.8 – 6 Mbit/s
Pitch: 5 – 25 Mbit/s

In case of DIGISTAT® configurations with no acquisition from medical devices, bandwidth occupation values are lower than those specified above.

4. Before starting

4.1 Installation and maintenance warnings

The following warnings provide important information on the correct installation and maintenance procedures of the DIGISTAT® product. They must be strictly respected.

!

Maintenance and repairs procedures shall be performed in compliance with Ascom UMS instruction only by Ascom UMS/Distributor technicians or personnel trained and authorized by Ascom UMS/Distributor.

!

It is recommended for the healthcare organization using the Product to stipulate a maintenance contract with Ascom UMS or an authorized Distributor. Part of the maintenance shall include the upgrade to the latest version available of the Product.

DIGISTAT® system must be installed and configured by specifically trained and authorized personnel. This includes ASCOM UMS (or authorized Distributor) staff and any other person specifically trained and authorized by ASCOM UMS/Distributor. Similarly, maintenance interventions and repairs on DIGISTAT® system must be performed according to ASCOM UMS guidelines only by ASCOM UMS/Distributor personnel or another person specifically trained and authorized by ASCOM UMS/Distributor.

!

DIGISTAT® system must be installed and configured by specifically trained and authorized personnel. This includes ASCOM UMS (or authorized Distributor) staff and any other person specifically trained and authorized by ASCOM UMS/Distributor.

- Use third party devices recommended by ASCOM UMS/Distributors.
- Only trained and authorized people can install third party devices.
- Incorrect installation of the third party devices can create a risk of injury to the patient and/or operators.
- Meticulously observe the manufacturer's instructions for the installation of third party hardware.
- Make provision for regular maintenance of the system according to the instructions present in this manual and those provided with the third party devices.

- The DIGISTAT® USB dongle must be stored and used in eligible environmental conditions (temperature, humidity, electromagnetic fields etc.), as specified by the dongle manufacturer. These conditions are equivalent to those required by common office electronic devices.

- Within the “Patient Area” (see Fig 1) it is recommended to use washable waterproof of devices.

- Within the “Patient Area” (see Fig 1) it is recommended to use washable, sterilizable rubber keyboards and mouse devices. For “touch screens” it is recommended to adopt capacitive technology (insensitive if used with gloves) because it discourages using gloves (sometimes contaminated).

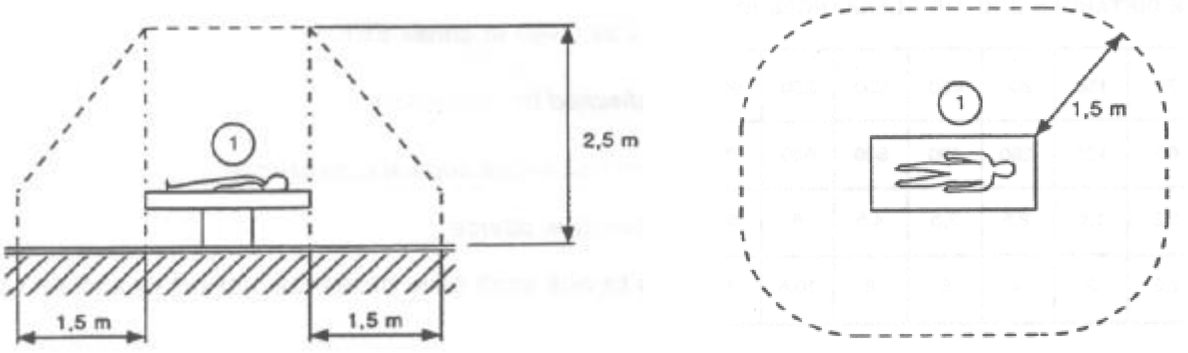


Fig 1 - Patient Area

4.1.1 Patient Area

The Patient Area is the space where there could be either intentional or unintentional contact between a patient and parts of the system (i.e. any device) or between a patient and other persons touching parts of the system (i.e. a physician who simultaneously touches a patient and other devices). The definition applies when the patient’s position is previously established; otherwise all possible patient positions must be taken into account.

According to IEC 60601-1 standard, every computer placed within the “Patient Area” must be a medical grade device.

According to the hardware license it is the responsibility of organization (individual, hospital or institution) to perform all the required measurements on the electrical safety of the electro-medical system in use (PC, display and other possible connected devices) taking full consideration of the environment in which they are used.

Should the Product be part of a “medical electrical system” through electrical and functional connection with medical devices, the healthcare organization is in charge of the required electrical safety verification and acceptance tests, even where ASCOM UMS performed in whole or in part the necessary connections.

4.2 Cleaning

Cleaning and disinfection procedures of hardware components must comply with the usual cleaning/disinfection procedures that the healthcare organization adopts for all the healthcare organization’s equipment (both fixed and moveable).

Check the suggested cleaning procedures in the manuals of the hardware products that are used alongside the DIGISTAT®system.

4.3 General precautions and warnings

To guarantee the reliability and security of the software during use, strictly observe the instructions given in this section of the manual.

Position all PCs appropriately to ensure adequate anterior and posterior ventilation. Failure to meet hardware ventilation requirements may cause equipment failure, thus jeopardizing patient data management system functions.

The Healthcare Organization shall ensure that the maintenance for the product and any third party device is implemented as requested to guarantee safety and efficiency and reduce the risk of malfunctioning and the occurrence of possible hazards to the patient and user.

! The Product shall be used only by trained and authorized clinicians.

4.3.1 Electrical safety

The hardware devices (PC, display, barcode reader, etc...) used together with DIGISTAT® system must comply with the relevant CE mark prescriptions, in particular with those indicated by the 2006/95/EC directive and subsequent amendments.

The device complies with the characteristics envisaged by the CE marking in accordance with directive 2006/95/EC and subsequent amendments.

! According to IEC 60601-1 standard, every computer placed within the “Patient Area” must be a medical grade device.

It is additionally recommended to perform all the relevant measurements on the leakage currents of the electro-medical system in use (PC, display and possible connected devices). The healthcare organization is responsible for these measurements.

! The healthcare Organization is responsible for all the required measurements on the electrical safety of the electro-medical system in use (PC, display and other possible connected devices) taking into consideration the actual environment in which the system is used.

4.3.2 Electromagnetic compatibility

The hardware devices (PC, display, barcode reader, etc...) used together with the DIGISTAT® system must comply with electromagnetic emission and immunity characteristics envisaged by the CE seal, in compliance with Directive 2004/108/EC and following amendments.

4.3.3 Devices eligibility

It is mandatory to use devices that are suitable for the environment in which they are installed and used (meeting, for instance, the directives LVD 2006/95/EC, EMC 2004/108/EC, penetration by liquids, etc.).

4.4 Privacy Policy

Appropriate precautions shall be taken in order to protect the privacy of users and patients, and to ensure that personal data is processed by respecting data subjects' rights, fundamental freedoms and dignity, particularly with regard to confidentiality, personal identity and the right to personal data protection.

'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

Special attention shall be dedicated to the data defined in "EU general data protection regulation 2016/679 (GDPR)" as "Special categories of personal data".

Special categories of personal data:
(…) Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and (…) genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Digistat® manages the following personal data:

- First name and surname
- Birthdate
- Sex
- Patient code
- Admission date
- Discharge date
- Patient weight
- Patient height

Digistat® can be configured to automatically hide this data on every application screen. To do that, on the Digistat® Configuration Application, set the system option named "Privacy Mode" to "true" (see the Digistat® configuration and installation manual for the detailed procedure). Its default value is "true".
If the "Privacy Mode" option is set to true, the following cases are possible:
- with no user logged in, no patient information is displayed.
- with a user logged in, and the user does not have a specific permission, no patient information is displayed.
- with a user logged in, and the user does have a specific permission, patient information is displayed.

The option can be applied to a single workstation (i.e. different workstations can be configured differently)

Please read the following precautions carefully and strictly observe them.

- The workstations must not be left unattended and accessible during work sessions. It is recommended to log out when leaving a workstation.

- Personal data saved in the system, such as passwords or users' and patients' personal data, must be protected from possible unauthorized access attempts through adequate protection software (antivirus and firewall). The healthcare organization is responsible for implementing this software and keep them updated.

Personal data can be present inside some reports produced by Digistat®. The healthcare organization needs to manage these documents according to the current standards on privacy and personal data protection.

Client workstations (both desktop and mobile) do not store patient data on disk. Patient data is stored only inside database and database storage depends on the healthcare structure's procedures and choices (examples: physical machine, SAN, virtualization environment). Patient data shall be treated according all the current standards on privacy and personal data protection.

Patient data is not stored in proprietary files. The only place in which patient data is stored is database.

In some circumstances, personal data are transmitted in non-encrypted format and using a connection which is not physically secure. An example of this kind of transmission are the HL7 communications. The healthcare organization is responsible for providing adequate security measures to comply with the local privacy laws and regulations.

! It is suggested to configure the database server so that the DIGISTAT® database is encrypted on the disk. To enable this option it is required SQL Server Enterprise Edition and during its installation it is necessary to enable the TDE (Transparent Data Encryption) option.

! The healthcare organization is in charge to provide basic training regarding privacy issues: i.e. basic principles, rules, regulations, responsibilities and sanctions in the specific work environment.
Ascom UMS/Distributor shall provide specialized training on the best use of the Product relating to privacy issues (i.e. database anonymization, privacy mode, user permissions etc.).

! The healthcare organization shall produce and keep the following documentation:

1) the updated list of the system administrators and maintenance personnel;
2) the signed forms of assignment and the certifications of attendance at the training courses;
3) a register of credentials, permissions and privileges granted to the users;
4) an updated list of the Product users.

! The healthcare organization shall implement, test and certify a procedure of automatic deactivation of no-more-active users after a certain period.

! The healthcare organization shall codify, implement and document a procedure for the periodic verification of belonging to the role of system administrator and technical maintenance personnel.

! The healthcare organization shall carry out audits and checks on the correct behavior of the operators.

4.4.1 User credentials features and use

This section explains the DIGISTAT® user credentials (username and password) features, their use and recommended policy.

- Every precaution must be taken in order to keep personal username and password secret.
- Username and password must be kept private. Do not let anybody know your username and password.
- Each user can own one or more credentials to access the system (username and password). The same username and password must not be used by more than one user.
- Authorization profiles must be checked and renewed at least once a year.
- It is possible to group different authorization profiles considering the similarity of the users' tasks.
- Each user account shall be linked with a specific person. The use of generic (for instance, "ADMIN" or "NURSE") must be avoided. In other words, for traceability reasons it is necessary that every user account is used by only one user.
- Each user has an assigned authorization profile enabling them to access only the functionalities that are relevant to their working tasks. The system administrator must assign an appropriate user profile when creating the user account. The profile must be reviewed at least once a year. This revision can also be performed for classes of users. The user profile definition procedures are described in the DIGISTAT® configuration manual.
- Password must be at least 8 characters.
- The password must not refer directly to the user (containing, for instance, user's first name, family name, date of birth etc.).
- The password is given by the system administrator at user account creation time. It must be changed by the user at first access in case this procedure is defined by configuration.

- After that, the password must be changed at least every three months.

- If username and password are left unused for more than 6 months they must be disabled. Specific user credentials, used for technical maintenance purposes, are an exception. See technical manual for the configuration of this feature.

- User credentials must also be disabled if the user is not qualified anymore for those credentials (it is the case, for instance, of a user who is transferred to another department or structure). A system administrator can manually enable/disable a user. The procedure is described in the DIGISTAT® configuration manual.

The following information is reserved to system administrators:

The password must match a regular expression defined in the DIGISTAT® configuration (default is ^........* i.e. 8 characters). The password is assigned by the system administrator when a new account for a user is created. The system administrator can force the user to change the password at first access to the system. The password expires after a certain (configurable) period, after that period, the user must change the password. It is also possible (by configuration) to avoid password expiration.

See DIGISTAT® configuration manual for detailed information on user account creation procedures and password configuration.

4.4.2 System administrators

ASCOM UMS/Distributor technical staff, when performing installation, updates and/or technical assistance may have access to and deal with personal sensitive data stored in the DIGISTAT® database.

For issues relating to management of personal sensitive data, ASCOM UMS/Distributor adopts procedures and working instructions complying with the current privacy regulation ("General Data Protection Regulation - EU 2016/679").

In performing the above mentioned activities ASCOM UMS/Distributor technical staff are setup as "System Administrator" for the DIGISTAT® system (see regulation of 25/11/2008 of the Privacy Guarantor on "System Administrators"). ASCOM UMS/Distributor staff performing this kind of procedures are appropriately trained on privacy issues and, in particular, in sensitive data treatment issues.

In order to comply with the requests of the "System Administrators" regulations, the responsible organization must:

- define nominal accesses;
- activate the access logs both at operating system and at client and at server level;

- activate the access logs to the database server Microsoft SQL Server (Audit Level);
- configure and manage all these logs to keep track of the accesses for at least one year.

4.4.3 System logs

DIGISTAT® records the system logs on the database. These logs are kept for a configurable period of time. Also, logs are kept for different times depending on their nature. Default times are:

- information logs are kept for 10 days;
- logs of warning messages are kept for 20 days;
- logs of alarm messages are kept for 30 days.

These times are configurable. See DIGISTAT® configuration manual for the configuration procedures.

4.5 Backup policy

It is recommended to regularly perform system backups.

The Healthcare Organization using DIGISTAT® system must define a backup policy that best suits its data safety requirements.

ASCOM UMS/Distributor is available to help and support in implementing the chosen policy.

The Healthcare Organization must ensure that backup files are stored in a way that makes them immediately available in case of need.

If data is stored on removable memory devices, the Healthcare Organization must protect these devices from unauthorized access. When these devices are not used anymore, they must be either securely deleted or destroyed.

4.6 Out of order procedure

It is recommended to perform the backup of the image of the systems, so that the replacement of the hardware allows to quickly restore the operating environment.

! Maintenance procedures and repairs shall be performed in compliance with Ascom UMS/Distributor procedures and guidelines and only by Ascom UMS/Distributor technicians or personnel specifically trained and explicitly authorized by Ascom UMS/Distributor.

This section describes the policy suggested by ASCOM UMS in case a DIGISTAT® workstation gets out of order. The goal of the procedure is to minimize the time required to successfully replace the out of order workstation.

ASCOM UMS suggests the healthcare organization has substitute equipment and an additional PC on which DIGISTAT® is already installed.

In case of a DIGISTAT® workstation is out of order, the substitute equipment can promptly replace the DIGISTAT® workstation.
Always remember that DIGISTAT® must only be installed by trained authorized personnel. This includes ASCOM UMS/Distributors staff and any other person specifically trained and explicitly authorized by ASCOM UMS/Distributor. Without an explicit, direct authorization from ASCOM UMS/Distributor, the healthcare organization staff are not authorized to perform installation procedures and/or to modify DIGISTAT® configuration.

The risk related to the DIGISTAT® workstation deactivation or substitution is that to associate the workstation with a wrong bed or room. This could lead to a “patient switch”, which is an extremely hazardous condition.

The risk related to the substitution and/or reconfiguration of network equipment involved in the DIGISTAT® data acquisition (i.e. port server, docking station, etc…) is that of assigning the acquired data to a wrong patient. The patient-acquired data relation is based on the IP address of the DIGISTAT® workstation. Changing it could lead either to data flow interruption or, in severe cases, to assigning data to the wrong patient.

! The out of order and replacement of a workstation is potentially hazardous. This is the reason why it must only be performed only by authorized and trained personnel.

The risk related to this procedure is that of associating a wrong bed/room/domain to the workstation, and therefore display data belonging to the wrong patients/beds.

In case a DIGISTAT® workstation needs to be deactivated and replaced, the hospital staff must promptly call ASCOM UMS (or authorized Distributors) and request the execution of this task.

ASCOM UMS suggests the healthcare organization defines a clear, univocal operating procedure and to share this procedure with all the staff members involved.

In order to speed up replacement times, ASCOM UMS suggests the healthcare organization has one or more substitution equipment with all the necessary applications already installed (OS, firewall, antivirus, RDP, ...) and with DIGISTAT® system already installed, but disabled (i.e. not executable by a user without the assistance of an ASCOM UMS technician). In case of out of order of a DIGISTAT® workstation, the substitution equipment availability assures the minimization of restoration times (hardware substitution) and reduces the risk of associating patient data incorrectly.

In case of out of order of a DIGISTAT® workstation we suggest to adopt the following procedure if a “substitution equipment” is available:

1) The healthcare organization’s authorized staff replaces the out of order PC with the “substitution equipment”
2) The healthcare organization staff calls ASCOM UMS/Distributor and requests the “substitution equipment” activation
3) The ASCOM UMS/Distributor staff disables the out of order workstation and correctly configure the “substitution equipment”
4) The out of order PC is repaired and prepared as “substitution equipment”

The instruction on how to enable/disable and replace a DIGISTAT® workstation, reserved to system administrators, is in the DIGISTAT® configuration manual.

4.6.1 Reconfiguration/substitution of network equipment

In case it is necessary to either reconfigure or substitute a network device involved in the DIGISTAT® data acquisition, the healthcare organization staff must promptly call ASCOM UMS/Distributor and schedule the substitution/reconfiguration procedure to allow ASCOM UMS staff to either reconfigure DIGISTAT® or provide all the necessary information to the healthcare organization. It is recommended, for this purpose, to define a clear procedure and share it with all the involved personnel. Some general indications about this are in the DIGISTAT® configuration manual.

4.7 Preventive maintenance

! Maintenance procedures and repairs shall be performed in compliance with Ascom UMS/Distributor procedures and guidelines and only by Ascom UMS/Distributor technicians or personnel specifically trained and explicitly authorized by Ascom UMS/Distributor.

It is suggested to perform the maintenance of DIGISTAT® system at least once a year. Maintenance frequency is a function of system complexity. In case of high complexity, it is suggested to perform maintenance more often, typically up to twice a year.

This is the maintenance checklist:

Preparatory checks

- DIGISTAT® system update necessity check.
- Check minimum requirements for a possible DIGISTAT® update (both hardware and software).
- Check the Server Service Pack version and state.
- Schedule the server/s restart to apply possible updates.
- Check the SQL Server Service Pack version and state.

```
SELECT SERVERPROPERTY('productversion'),
SERVERPROPERTY ('productlevel'),
SERVERPROPERTY ('edition')
```

- Schedule possible updates with the technical staff

Checks to be performed

Antivirus

- Check that Antivirus Software is installed and updated (both the application and the virus list definition).
- If viruses are present, inform the competent technician and, if authorized, try to clean the PC.

Database

- Check that an effective DIGISTAT® database clean-up and backup policy is configured.
- Check that the clean-up and back-up store procedures exist (UMSBackupComplete, UMSBackupDifferential, UMSCleanLog, UMSCleanDriver) and the related schedule.
- Check that back-up files exist (both full and differential).
- Check with the healthcare organization technical department that backup, configuration folders and data folders are correctly copied to another storage device.
- Using a previous backup, restore the database to verify its correctness.
- Delete the old back-up files (.bak) and the possible files that are not inherent to DIGISTAT® configuration on the network shared path.
- Check that the other jobs on SQL Agent or scheduled tasks (for instance those that are support to integration with third-parties systems) are present, and that their schedule is adequate.

- On SQL Agent check that the different JOBs are executed and that there are not hanging JOBs or JOBs in error.
- Check the SQL Server LOGs.
- Check the database total size and the number of records in the main tables. Script for checking all the tables size:

```
USE [DATABASENAME]
GO

CREATE TABLE [#SpaceUsed]
(
  [name] [nvarchar](250) NULL,
  [rows] [nvarchar](250) NULL,
  [reserved] [nvarchar](250) NULL,
  [data] [nvarchar](250) NULL,
  [index_size] [nvarchar](250) NULL,
  [unused] [nvarchar](250) NULL
) ON [PRIMARY]

DECLARE @INS AS nvarchar(MAX)
SET @INS = '';

SELECT @INS = @INS + 'INSERT INTO #SpaceUsed exec sp_spaceused '''
+ TABLE_NAME + '''; '
FROM INFORMATION_SCHEMA.TABLES
WHERE TABLE_TYPE = 'BASE TABLE'
ORDER BY TABLE_NAME

EXEC (@INS);

SELECT *
FROM #SpaceUsed
ORDER BY CAST([rows] AS INT) DESC

DROP TABLE [#SpaceUsed]
```

Server

- Check the Windows™ server event log.
- Check the permissions on the shared folders (e.g. Backup folder).
- File and directories no longer needed should be removed to free up space on server disk.
- Check the displays (if any) on the server rack and verify that there are neither visual nor sound alarms.
- Check that on the different disk units there is enough space available.
- Disk check with dedicated tools (checkdisk, defrag, etc.).
- In case there are disks in RAID, check the health conditions of the RAID unit on the RAID management software.
- Check the LED of the non-alarmed RAID units.
- If an UPS (Uninterruptible Power Supply) is connected, check its health conditions with its management software.
- In case of UPS schedule an electric interruption (an electric failure simulation) and check that the server is configured to perform a CLEAN shutdown.

Workstations

- Check if the Regional Settings on the workstations are appropriate with the DIGISTAT® installation language.
- Check if every workstation has a default printer.

DIGISTAT® system

- Check data presence (SELECT) Patient, Admission, Bed, Location tables and some random others.
- Check on the network table that no workstation has the ALL value in the "modules" field.
- Check, and if appropriate, clean the service and/or ASCOM UMS Gateway LOG.
- Check, and if appropriate, clean the DAS LOGs for the Drivers (if enabled).
- Check that the privacy policy is respected as stated in this manual in paragraph 4.4.

Connection to devices

- Check the connections (cables and wiring system) with data acquisition devices.

Instruction for use

- Check that the user documentation in PDF format (PDF provided together with the product) is present on the server and appropriate with DIGISTAT® version.
- Check that the folder containing the user documentation in electronic format on the server is accessible to DIGISTAT® users.
- Check that the HELP button opens the user documentation.
- Check that all the other contents provided by ASCOM UMS and integrated in the HELP of DIGISTAT® system are updated.

4.8 Compatible devices

Please contact ASCOM UMS/Distributor for the list of available drivers.

4.9 System unavailability

If during start up there are problems connecting to the server the system provides a specific information message.

The connection problem is often automatically solved in a short time. If it does not happen, it is necessary to contact the technical assistance (see section 8 for the contacts list).

In rare, often extreme cases, it may be physically impossible to use the DIGISTAT® system, for example cases of natural disasters, or long black outs.

It is responsibility of the healthcare organization using DIGISTAT® to define an emergency procedure to put into effect in those cases. This is necessary to

1) Make it possible for the departments to keep on working
2) Restore as soon as possible the system to full availability (back-up policy is part of this management. See paragraph 4.5).

! It is responsibility of the healthcare organization using DIGISTAT® to define an emergency procedure to put into effect in case of system unavailability.

ASCOM UMS/Distributor offers full support for the definition of such procedure.

See section 10 for the contacts list.

5. DIGISTAT® Mobile

Digistat® Mobile is a mobile application designed to bring some of the DIGISTAT® suite functionalities directly “in the hands” of nurses and clinicians. DIGISTAT® Mobile acts as a container for a set of modules, each one designed to provide specific information and presenting it to the staff in a clear and concise way.

5.1 Information for the user

Please read carefully the following warnings.

!	In case of disconnection of the DIGISTAT® Mobile application a specific notification is generated, consisting of a characteristic and persisting sound and vibration. Sound duration is configurable. The sound is repeated until the connection is reestablished. Connection is automatically reestablished as soon as possible.

!	The mobile device shall always be kept by the user either in direct contact or close enough to be clearly audible.

!	The DIGISTAT® Mobile application may display personal and/or confidential information. It is therefore recommended to not leave unattended the handheld device on which the DIGISTAT® Mobile application runs or, in case, to always logout before leaving it unattended.

!	DIGISTAT® Mobile can be closed by the user. After which time the application will not send any other notification.

!	Because of the Android architecture, in exceptional cases, which are hard to foresee, the operating system can close the DIGISTAT® Mobile application. After such event, the application will not send any other notification.

! If the generic Alaris® Driver is in use it is necessary to wait at least ten seconds after disconnecting an infusion pump before connecting another.

! The update of data displayed on screen caused by device connection, power off, disconnection and change of status depends on the time required by the device itself to communicate the changes. This time depends on various factors. Among them is the device type and type of connection. For some devices, there are conditions in which the delay in communicating changes might be important. Since they might change depending on devices configuration and operational conditions, it is not possible to provide an indication of the delays for all the possible devices

! The mobile device shall support the vibration mode.

! Check that the medical devices are correctly connected by verifying that their data are displayed on the Smart Central Mobile.

! Use the sound check procedure to verify if the audio on the workstation/handheld device is correctly working (see related paragraph for the procedure).

! On the connected medical device where it is possible, generate an artificial alarm condition to verify that the corresponding alarm notification is correctly displayed on the Smart Central Mobile (it is suggested to perform this check at least once per shift).

! Within the Smart Central Mobile Application the alarms are grouped in “physiological alarms”, “technical alarms” and “other”. This kind of differentiation has no impact on the way the alarms are displayed on the Smart Central Mobile interface.

! The drivers used to read the data from the connected medical devices have a reading-cycle of less than 3 seconds (i.e. all the data from the devices is read every 3 seconds at maximum). However, there are devices that communicate the information less frequently (5-10 seconds interval). Refer to the specific driver documentation for details on the reading-cycle.
As soon as a driver detects an alarm, it takes maximum 1 second to transfer it to the Smart Central Mobile.

! In case of electrical black-out, it takes a few minutes for the system to be fully operative again and therefore generate alarm notifications (usually this time is less than 3 minutes, however it depends on the configuration of the used computers).

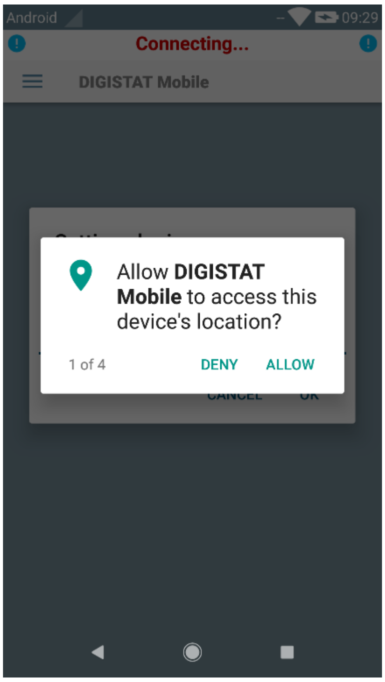
5.2 Start-up

Although the contents are the same, start-up and layout are slightly different on the ASCOM Myco device (if integrated with ASCOM Unite) and other Android handheld devices (or ASCOM Myco not integrated with ASCOM Unite).
The layout displayed in Fig 8 is referring to a scenario where the ASCOM Myco is integrated with UNITE.

5.2.1 Authorizations for proper functioning

In order to perform the expected functioning, the DIGISTAT® Mobile application at its first use asks to provide some basic authorizations. All the requested authorization have to be provided.

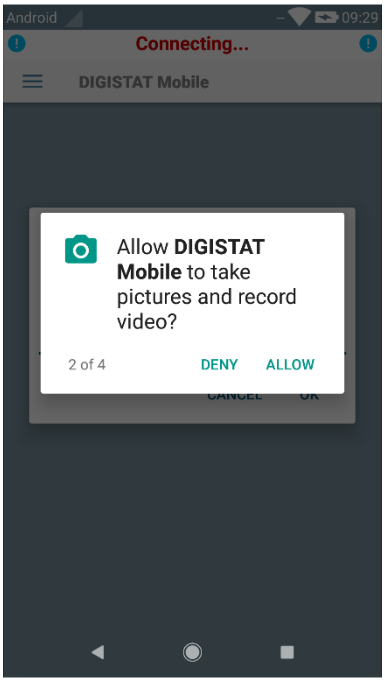
In Fig 2 is reported the screen shown to ask the user the authorization to access the device’s location. The user has to tap the label “Allow”:



Allow **DIGISTAT Mobile** to access this device's location?

Fig 2

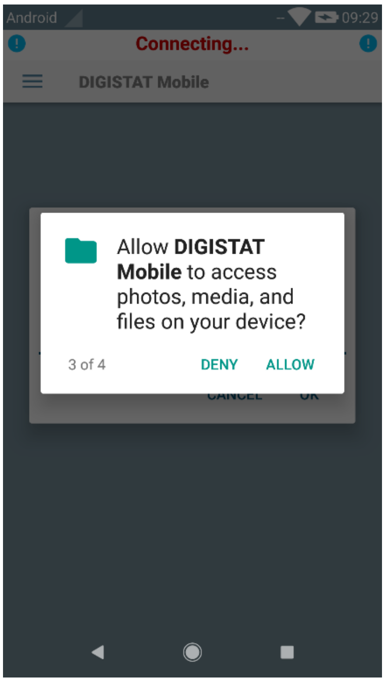
In Fig 3 is reported the screen shown to ask the user the authorization to take pictures and record video. The user has to tap the label “Allow”:



Allow **DIGISTAT Mobile** to take pictures and record video?

Fig 3

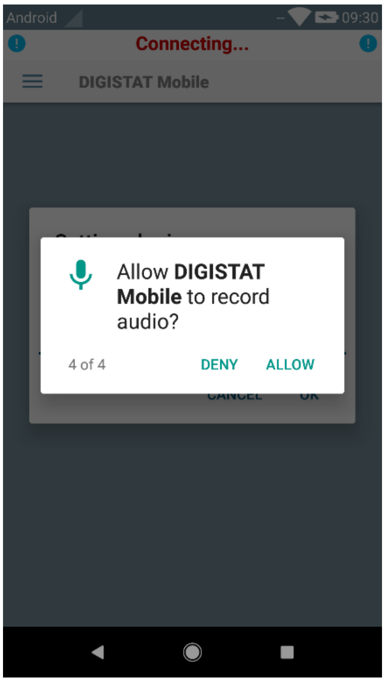
In Fig 4 is reported the screen shown to ask the user the authorization to access photos, media and files on the device. The user has to tap the label “Allow”:



Allow **DIGISTAT Mobile** to access photos, media, and files on your device?

Fig 4

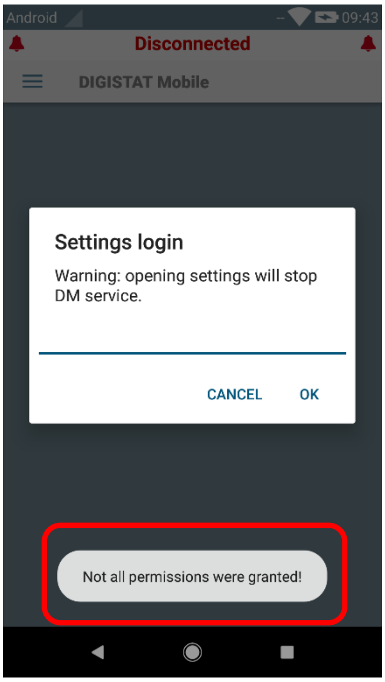
In Fig 5 is reported the screen shown to ask the user the authorization to record audio. The user has to tap the label “Allow”:



Allow **DIGISTAT Mobile** to record audio?

Fig 5

If at least one of the requested authorization is not granted, the DIGISTAT® Mobile application raises a toast message for the user (Fig 6):



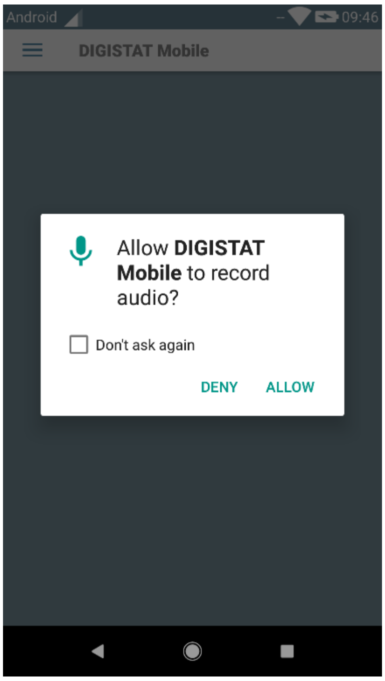
Settings login

Warning: opening settings will stop DM service.

Not all permissions were granted!

Fig 6

In addition, once the configuration of the system is correctly performed (see Paragraph 5.2.1) the DIGISTAT® Mobile application asks again to provide the missing authorization (Fig 7):



Allow **DIGISTAT Mobile** to record audio?

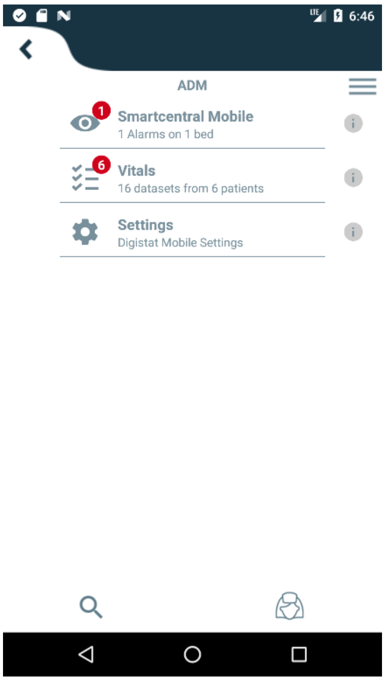
□ Don't ask again

Fig 7

If the requested authorization is again not granted, the DIGISTAT® Mobile application raises furthermore the same toast message for the user shown before (Fig 6):

5.2.2 ASCOM MYCO (w/ Unite) Start-Up

On the ASCOM Myco device, when integrated with ASCOM Unite, the DIGISTAT® Mobile application is already running on the rightmost page of the Myco's Unite launcher.



Smartcentral Mobile
1 Alarms on 1 bed

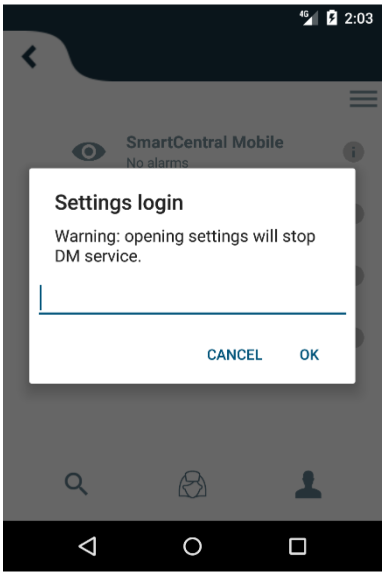
Vitals
16 datasets from 6 patients

Settings
Digistat Mobile Settings

Fig 8

The available modules are listed on the page. Touch the row corresponding to the module to open it.

The **Settings** option makes it possible to access some configuration options. A specific password is required to access this area (Fig 9).

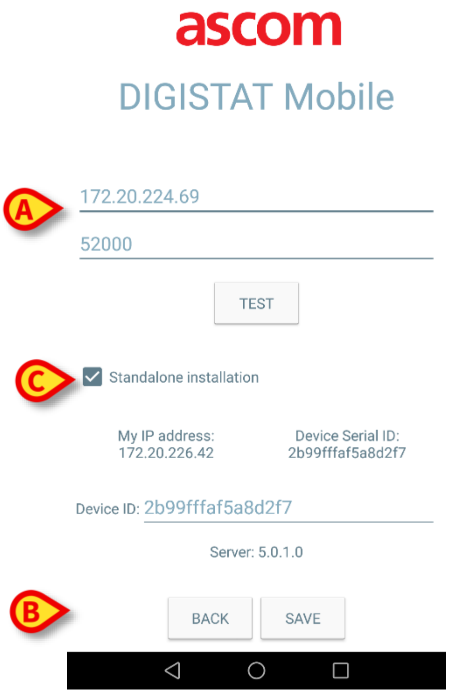


Settings login

Warning: opening settings will stop DM service.

Fig 9

- ➢ Insert password and touch **OK** to access these options. The following screen will be displayed.



172.20.224.69

52000

☑ Standalone installation

My IP address: 172.20.226.42

Device Serial ID: 2b99fffaf5a8d2f7

Device ID: 2b99fffaf5a8d2f7

Server: 5.0.1.0

Fig 10

If ASCOM-Unite integration is used, please deselect the checkbox in Fig 10 **C**.

It is here possible to specify the IP address of the server and the server port (Fig 10 **A**).

After editing:

- ➢ touch the **Test** button to test the new settings
- ➢ touch the **Save** button to save the changes made,

The lower field (Device ID - Fig 10 **B**) makes it possible to change the device id code. Since the Device ID is changed, to recover the default value the user has to do the following steps:

- ➢ Insert an empty value in Fig 10 **B** and then save.
  The Digistat application will signal by means of a cyclical toast message that the Device ID is empty;
- ➢ Access again to Settings screen (Fig 10) as above explained.

The default Device ID is now recovered (Fig 10 **B**).

5.2.3 Android device start-up

On the handheld device,

- ➢ Touch the 🖐 icon.

The following screen will be displayed (Fig 11).

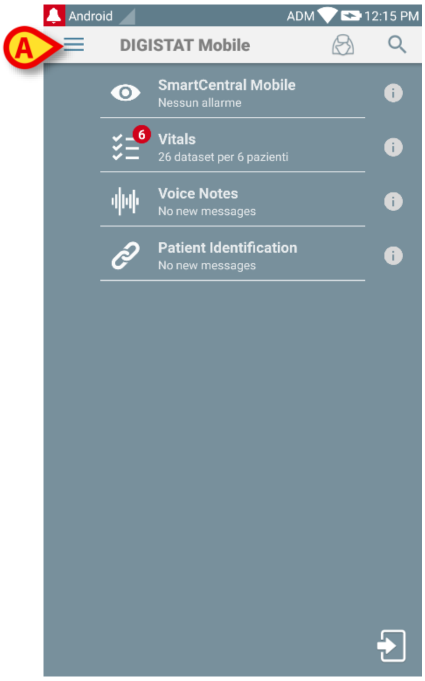


Fig 11

The available modules are listed on the page. Touch the row corresponding to the module to open it.

- To access the “Settings” area, touch the ☰ icon on the top-left corner.

The following options will open (Fig 12 - see paragraph 5.3 for the full list of options).

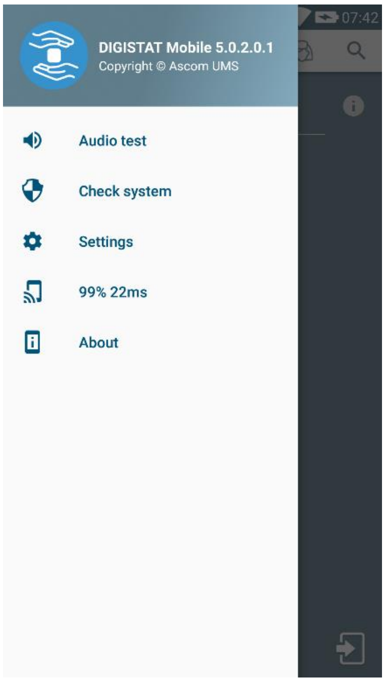
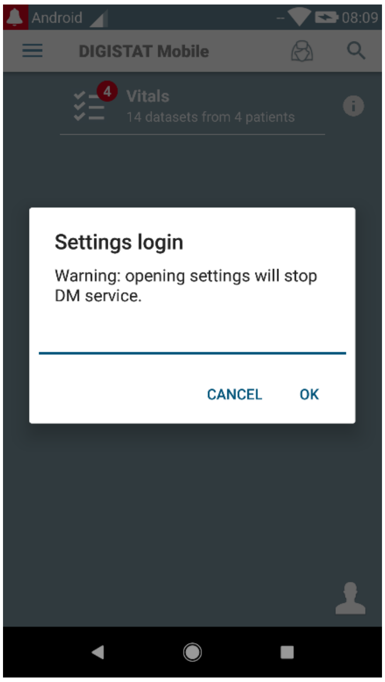


Fig 12

- Touch **Settings** to access the settings management screen. A specific password is required to access this area.



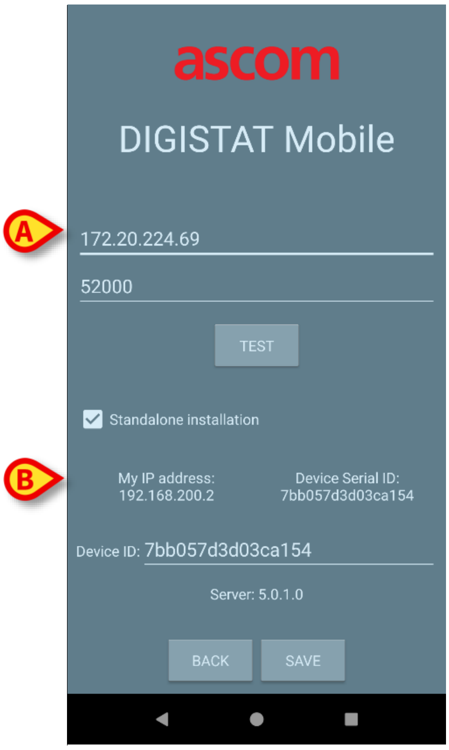
Settings login

Warning: opening settings will stop DM service.

CANCEL OK

Fig 13

- ➢ Insert password and touch **OK** to access these options. The following screen will be displayed.



172.20.224.69

52000

☑ Standalone installation

My IP address: 192.168.200.2

Device Serial ID: 7bb057d3d03ca154

Device ID: 7bb057d3d03ca154

Server: 5.0.1.0

Fig 14

It is here possible to specify the IP address of the server and the server port (Fig 10 **A**). After editing:

- ➢ touch the **Test** button to test the new settings
- ➢ touch the **Save** button to save the changes made,

The lower field (Device ID - Fig 14 **B**) makes it possible to change the device id code. Since the Device ID is changed, to recover the default value the user has to do the following steps:

- ➢ Insert an empty value in Fig 14 **B** and then save.
  The Digistat application will signal by means of a cyclical toast message that the Device ID is empty;
- ➢ Access again to Settings screen (Fig 14) as above explained.

The default Device ID is now recovered (Fig 14 **B**).

5.2.4 Updates installation (APK files)

Whenever a software update is available, an additional row is displayed on the start page.

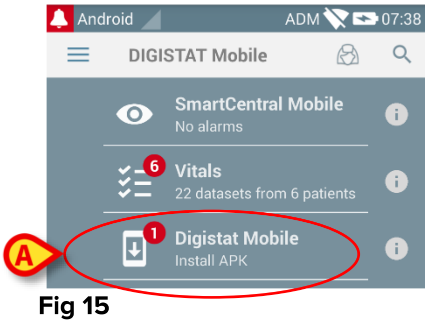


Fig 15

To install the software updates

- ➢ Touch the row indicated in Fig 15 **A**.

5.3 Lateral Menu

NOTE: the lateral menu is only available on devices not connected with UNITE.

The ☰ icon on the top-left corner opens a menu containing different options (Fig 16).

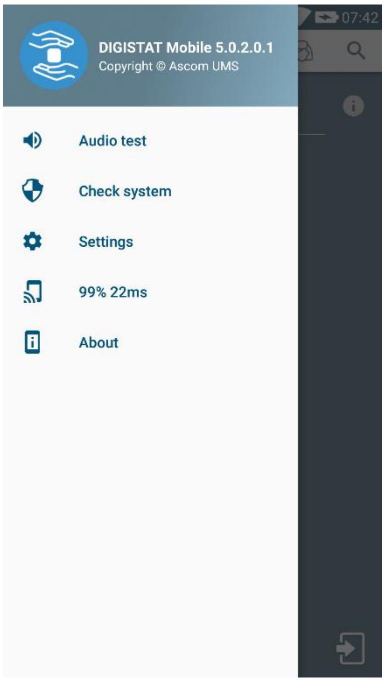


Fig 16

These are:

Audio test

Touch the **Audio Test** button to test the sound-vibration associated to the notifications (see paragraph 5.6.1).

Check system

Touch this item to verify if all required authorization allowing the proper functioning of the Digistat Mobile Applications are provided by the user.

Settings

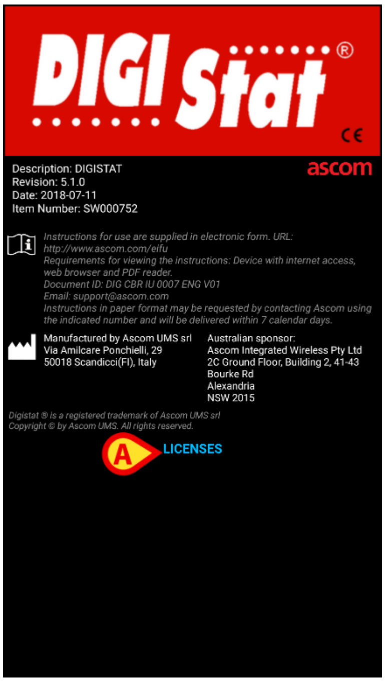
Touch this option to access the Settings screen (see previous paragraph 5.2.3).

Wireless connection status

Indicating the wireless connection status.

About

Touch this option to open a screen containing general info about Digistat® Product and Manufacturer. Touch **Licenses** on this screen (Fig 17 **A**) to display the licenses associated with the Product.



Description: DIGISTAT
Revision: 5.1.0
Date: 2018-07-11
Item Number: SW000752

Instructions for use are supplied in electronic form. URL: http://www.ascom.com/eifu
Requirements for viewing the instructions: Device with internet access, web browser and PDF reader.
Document ID: DIG CBR IU 0007 ENG V01
Email: support@ascom.com
Instructions in paper format may be requested by contacting Ascom using the indicated number and will be delivered within 7 calendar days.

Manufactured by Ascom UMS srl
Via Amilcare Ponchielli, 29
50018 Scandicci(FI), Italy

Australian sponsor:
Ascom Integrated Wireless Pty Ltd
2C Ground Floor, Building 2, 41-43
Bourke Rd
Alexandria
NSW 2015

Digistat ® is a registered trademark of Ascom UMS srl
Copyright © by Ascom UMS. All rights reserved.

Fig 17

5.4 Login

To login to DIGISTAT® Mobile

➢ Touch **Login** on the lower-right corner of the "Applications list" screen (Fig 18 **A**)

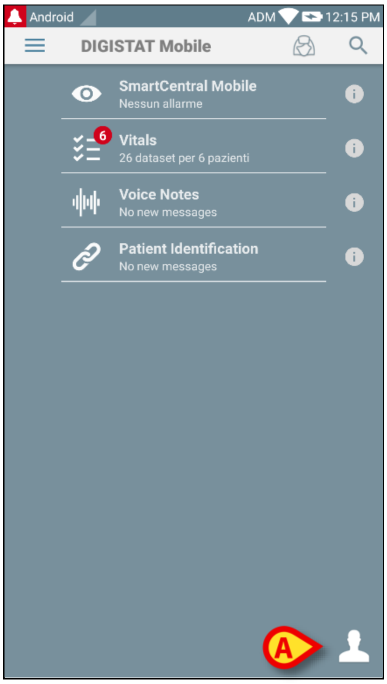


Fig 18

The following screen will be displayed (Fig 19)

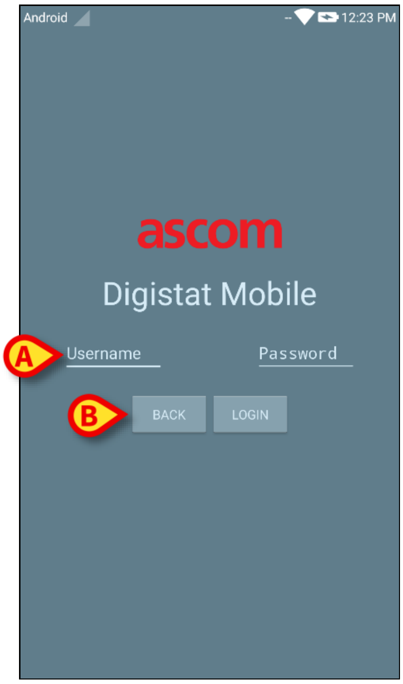


Fig 19

- ➢ Insert username and password (Fig 19 **A**).
- ➢ Touch the **Login** button (Fig 19 **B**)

The acronym indicating the logged user will then be displayed either on the “Applications list” screen (for Myco/UNITE version - Fig 20 **A**),

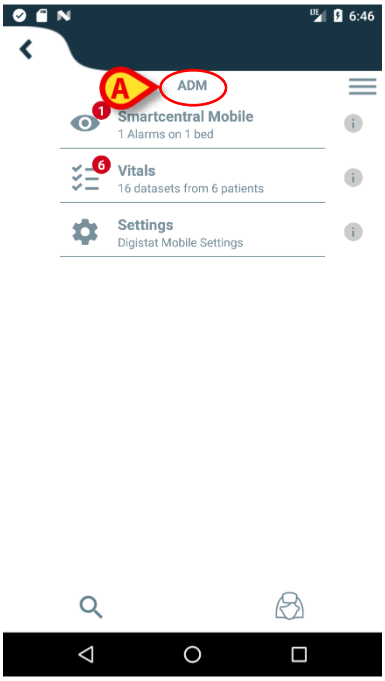


Fig 20

or on the upper notification bar (for other android handheld devices - Fig 21 **A**).

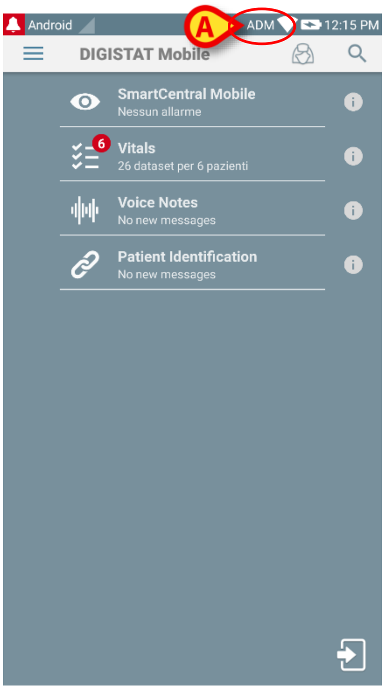


Fig 21

5.5 Upper notification bar

The upper notification bar (Fig 22 **A**) is always visible and displays general information.

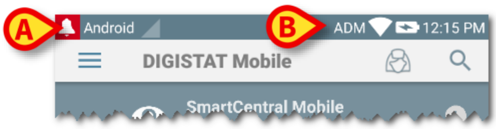


Fig 22

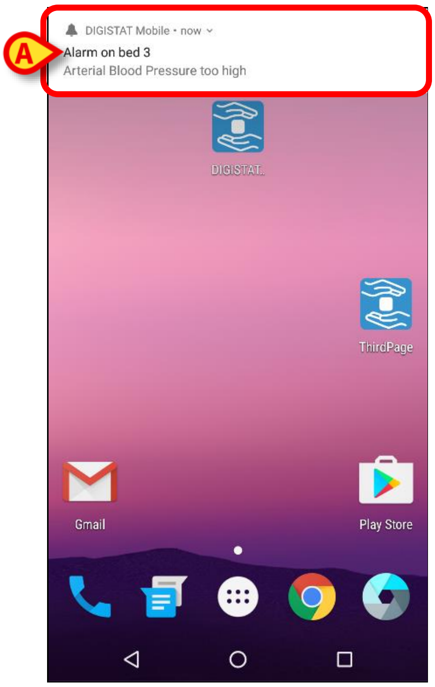
The red bell icon placed on the top-left corner (only visible in non-Myco/UNITE devices 🔔 - Fig 22 **A**) is displayed if there are notifications for one of the patients, coming from any module. It is as well displayed if the module is not active.

On the top-right corner the following information is displayed (Fig 22 **B**):

- Acronym of the logged user (non-Myco/UNITE devices);
- Wi-fi connection status;
- Battery charge status;
- Time.

5.6 General System Notifications

DIGISTAT® Mobile provides short notifications of alarms/messages coming from any installed module when the application is not active as well (Fig 23 **A**). The highest level notification indicates the overall alarm level of the Digistat® Mobile application.
For each module a row in the notification area is foreseen. Any change in the notifications is performed within the row related to the module triggering notification change.


DIGISTAT Mobile • now

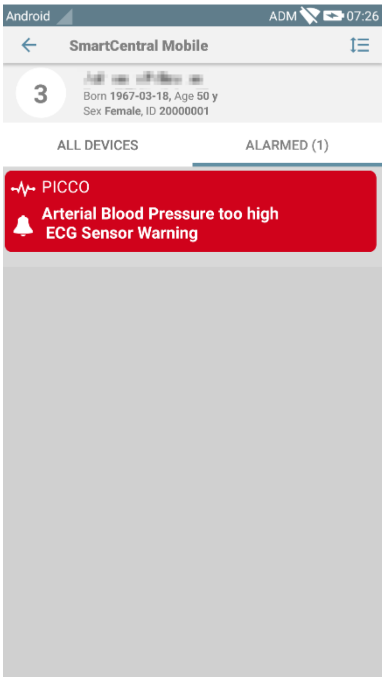
Alarm on bed 3

Arterial Blood Pressure too high

Fig 23

- ➢ Swipe the notification to make it disappear.

- ➢ Touch the notification to directly access the relevant module/patient (see an example in Fig 24; see further paragraphs for a description of the specific modules). If the alarm notification from a module is related to one patient, then by touching it the alarmed patient tab is displayed; moreover, if the alarm notification is raised for more than one patient, by touching it the list of alarmed patient is displayed.


SmartCentral Mobile

3 [redacted]

Born 1967-03-18, Age 50 y

Sex Female, ID 20000001

ALL DEVICES ALARMED (1)

PICCO

Arterial Blood Pressure too high

ECG Sensor Warning

Fig 24

In addition to screen notifications, the Product is able to handle sound notifications by means of the device speaker and light notifications by means of the notification led.

In the case of sound notifications, the Product ever plays the notification with higher priority; if a notification is being executed and a new alarm has to be raised, then the Product restarts the notification with higher priority.

In the case of light notifications, the notification led results in the color related to the higher priority notification i.e. the alarm level of the whole Digistat® Mobile application.

5.6.1 Sound Check procedure

! The Sound Check procedure shall be performed at least once per shift.

The Sound Check Procedure makes it possible to verify if the sound notification of alarms is working properly.

To perform the "Sound Check" procedure

- Activate the main screen of Digistat® Mobile application (Fig 25).

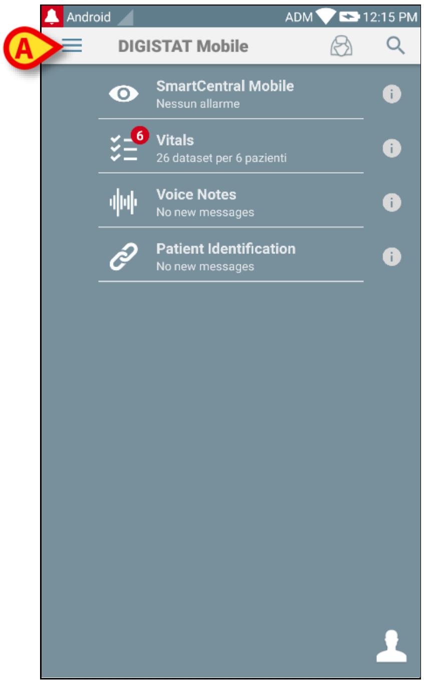


Fig 25

- Touch the ≡ icon on the top-left corner of the screen (Fig 25 **A**)

The following menu will be displayed (Fig 26).

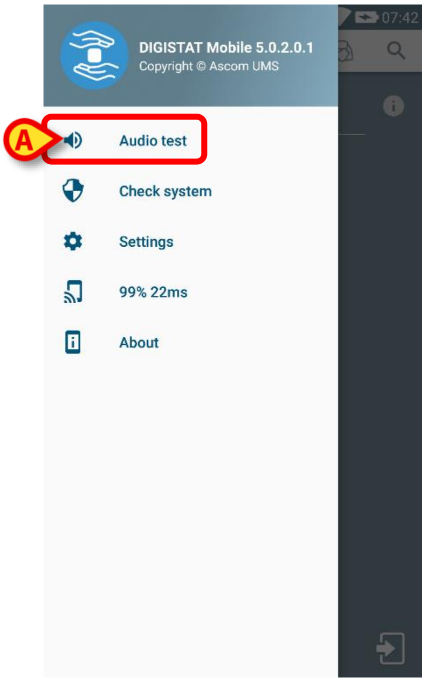
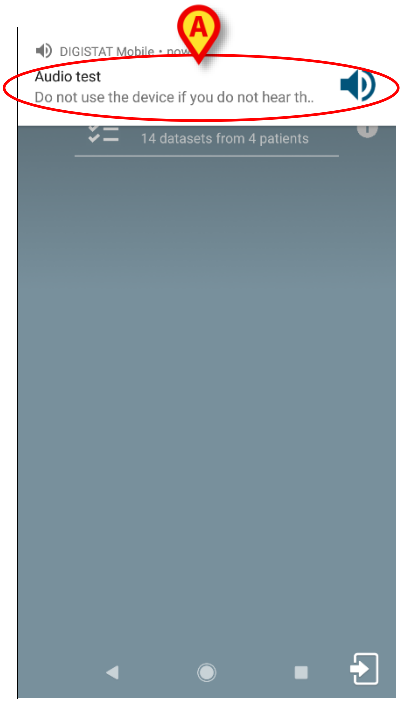


Fig 26

➢ Touch the **Audio test** option (Fig 26 **A**).

A test notification/sound will be this way provided (Fig 27 **A**).



Audio test
Do not use the device if you do not hear th..

Fig 27

!

Do not use the device if you do not hear the alarm sound and/or feel the device vibration.

5.6.2 Check System procedure

The Check System menu item checks if all the authorization required from Digistat Mobile application to work properly were correctly provided since the application was installed. In addition, the proper firmware version of the device is also checked.

In the Paragraph 5.2.1 were described the authorization requested for the proper functioning of the DIGISTAT® Mobile application.

To perform the Check System

- ➢ Activate the main screen of Digistat® Mobile application (Fig 28).

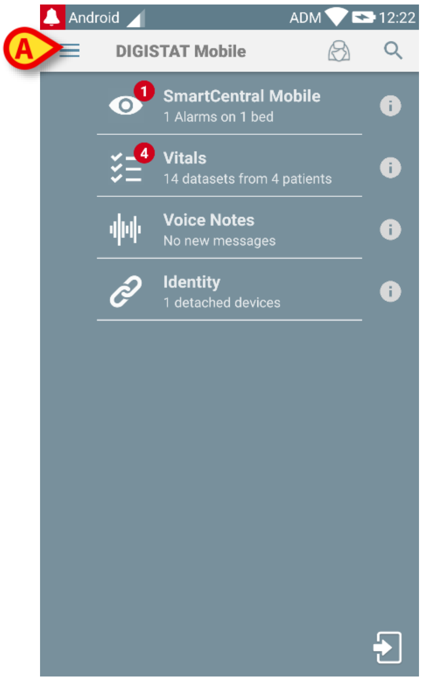


Fig 28

- ➢ Touch the ☰ icon on the top-left corner of the screen (Fig 28 **A**)

The following menu will be displayed (Fig 29).

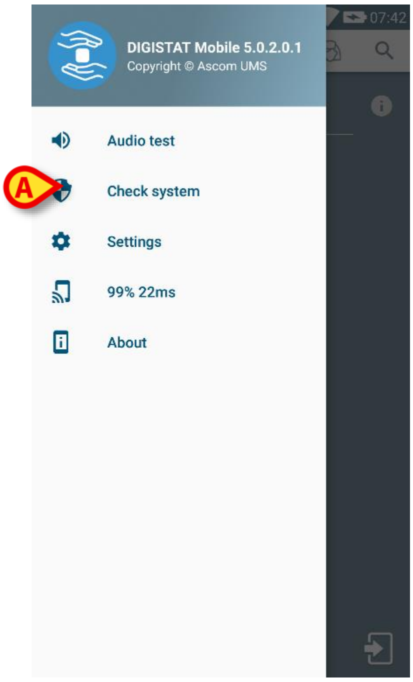
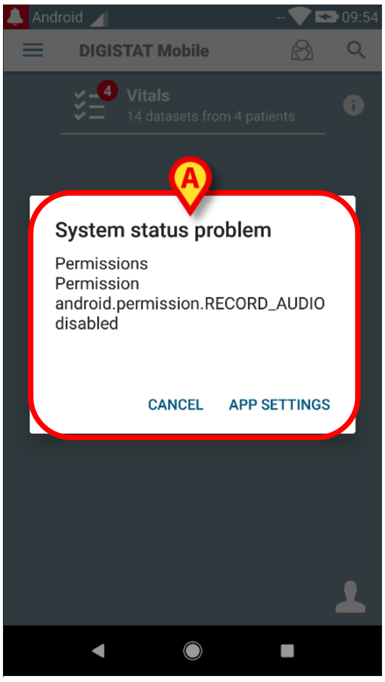


Fig 29

- ➢ Touch the **Check System** option (Fig 29 **A**).

A test notification will be this way provided, showing a reference to the missing authorizations (Fig 30 **A**). Please provide the requested authorization.



System status problem

Permissions
Permission
android.permission.RECORD_AUDIO
disabled

Fig 30

In addition to the above mentioned checks, the Check System raises an alert message to the user if the timestamp of Mobile client differs from the one of Mobile server.

Because on some devices an aggressive battery optimization policy is in place, foreground services might be frozen: this may also occur to Digistat applications. The Check System procedure is additionally in charge to verify that Digistat Applications are in the battery optimization whitelist:

- Since this check has a negative result, a message is raised to the user suggesting to insert Digistat in the battery optimization whitelist.

! Do not use the device if you do not have previously provided all the requested authorizations.

5.7 Patient's search functionalities

The system implements several patients search tools. These tools can be accessed from the Patients List screen.

To access the search functionalities

- Touch the icon indicated in Fig 31 **A** for devices without Myco/Unite integration or in Fig 32 **A** for devices with Myco/Unite integration.

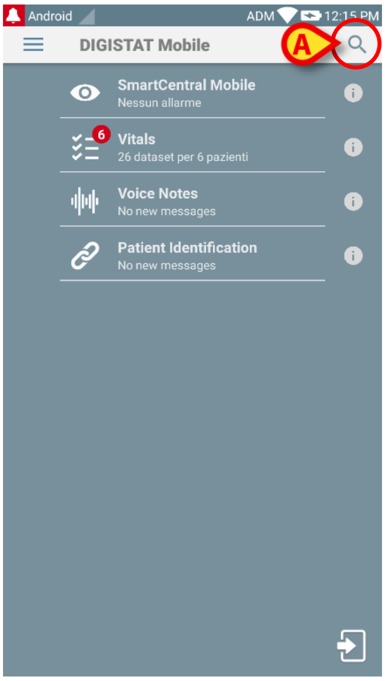


Fig 31

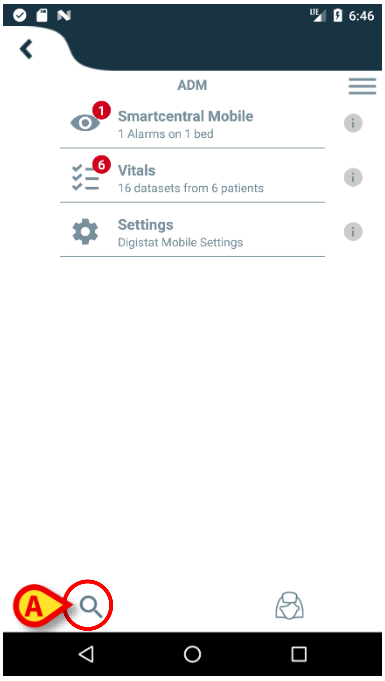


Fig 32

The following screen will open (Fig 33).

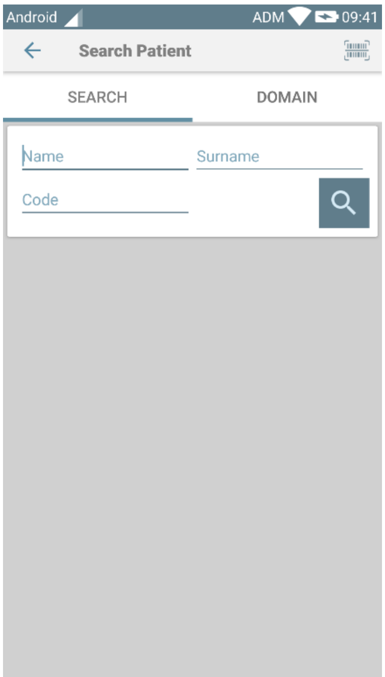


Fig 33

Three search options are available:

1. Textual search (see paragraph 5.7.1);
2. Barcode scan (see paragraph 5.7.2);
3. NFC code scan (see paragraph 5.7.3).

5.7.1 Textual search

- Insert patient data in the fields indicated in Fig 34 **A** (name, surname, code), then click the **Search** button (Fig 34 **B**). Partial information is allowed.

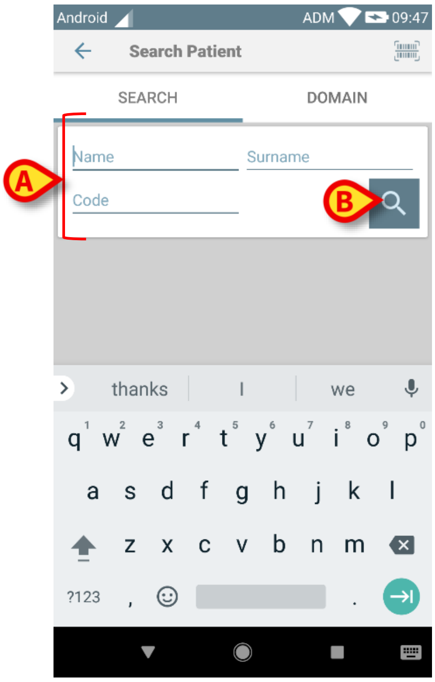
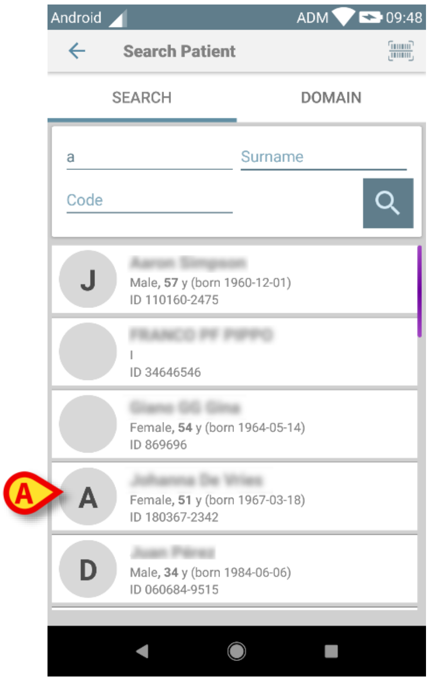


Fig 34

The list of patients whose data match those specified will be displayed (Fig 35).



J [redacted]
Male, 57 y (born 1960-12-01)
ID 110160-2475

[redacted]
I
ID 34646546

[redacted]
Female, 54 y (born 1964-05-14)
ID 869696

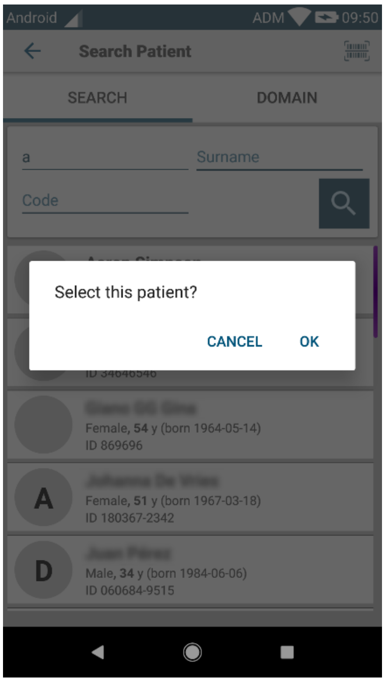
A [redacted]
Female, 51 y (born 1967-03-18)
ID 180367-2342

D [redacted]
Male, 34 y (born 1984-06-06)
ID 060684-9515

Fig 35

The search is performed among all patients, both belonging and not belonging to the device domain. If the patient is currently in bed, the bed number is displayed on the left.

- ➢ Touch the box corresponding to a patient to select the patient. User confirmation is required (Fig 36).



Android ADM 09:50

Search Patient

SEARCH DOMAIN

a Surname

Code

Select this patient?

CANCEL OK

ID 34646546

[redacted]
Female, 54 y (born 1964-05-14)
ID 869696

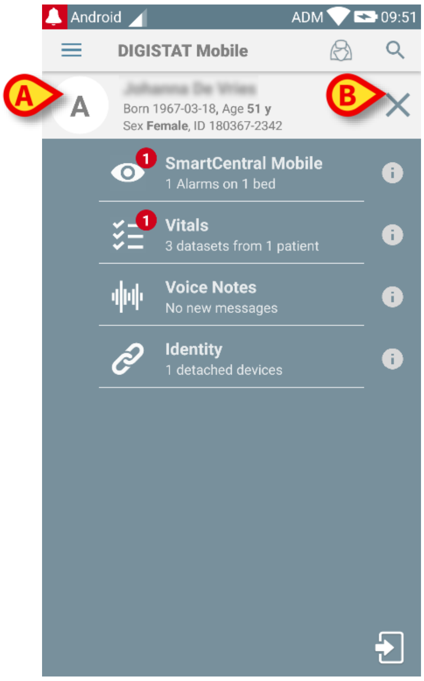
A [redacted]
Female, 51 y (born 1967-03-18)
ID 180367-2342

D [redacted]
Male, 34 y (born 1984-06-06)
ID 060684-9515

Fig 36

- ➢ Touch **Ok** to confirm.

The patient will be this way selected (Fig 37).



Android ADM 09:51

DIGISTAT Mobile

A [redacted]
Born 1967-03-18, Age 51 y
Sex Female, ID 180367-2342

SmartCentral Mobile
1 Alarms on 1 bed

Vitals
3 datasets from 1 patient

Voice Notes
No new messages

Identity
1 detached devices

Fig 37

Patient data are on top of the page (Fig 37 **A**). All the data in all the DIGISTAT® Mobile modules are now filtered by patient (i.e. all and only the selected patient alarms/notifications are displayed).

- ➢ Touch the cross indicated in Fig 37 **B** to deselect the patient and turn to “All Patients” mode again.

5.7.2 Barcode Scan search

The Barcode Scan functionality makes it possible to select a patient by scanning his/her code.

To access the Barcode Scan functionality

- ➢ Access the search page as described in paragraph 5.6.2.
- ➢ Touch the ▥ icon indicated in Fig 38 **A**.

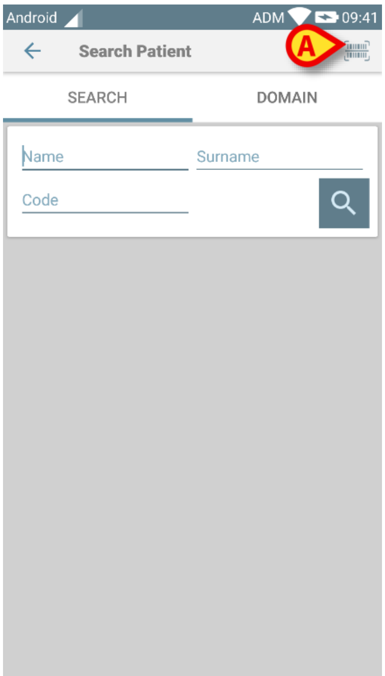


Fig 38

The device camera will be in this way activated.

- ➢ Scan the wanted patient's barcode.

The patient will be this way selected. The screen shown in Fig 37 (example) will be displayed.

5.7.3 NFC Reader search

The NFC Scan makes it possible to select a patient using the device's own Near Field Communication sensor.

To do that:

- ➢ Access the search page as described in paragraph 5.6.2.

The device NFC reader will be this way activated.

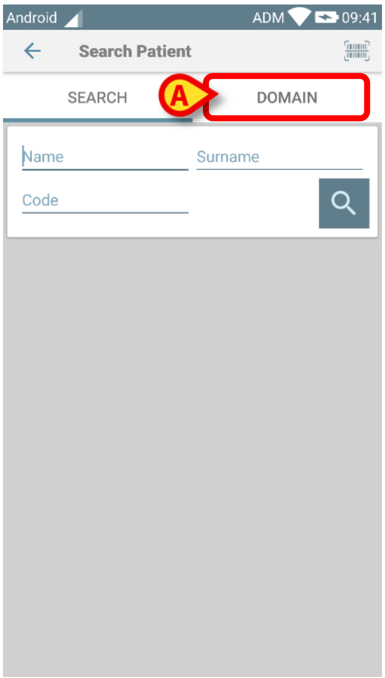
- Position the device close to the patient’s Tag.

The patient will be this way selected. The screen shown in Fig 37 will be displayed.

5.7.4 Single Patient Selection

To select a single patient:

- ➢ Touch the icon indicated in Fig 31 **A** for devices without Myco/Unite integration or in Fig 32 **A** for devices with Myco/Unite integration. The following screen will appear (Fig 39 **A**):



Android ADM 09:41

Search Patient

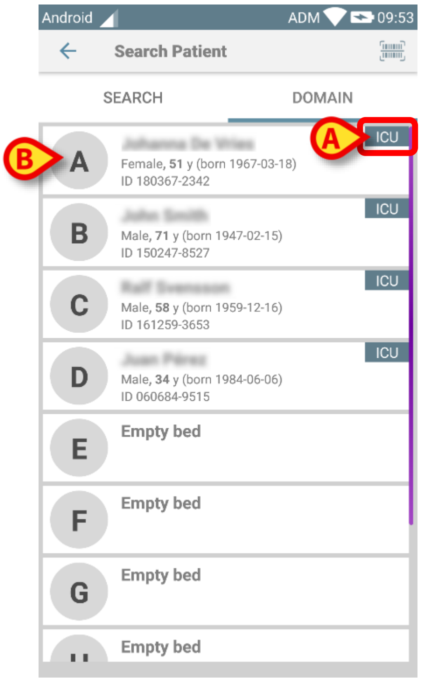
SEARCH DOMAIN

Name Surname

Code

Fig 39

- ➢ Touch the "**DOMAIN**" tab. The following window shall appear (Fig 40)



Android ADM 09:53

Search Patient

SEARCH DOMAIN

A [redacted] Female, 51 y (born 1967-03-18) ID 180367-2342 ICU

B [redacted] Male, 71 y (born 1947-02-15) ID 150247-8527 ICU

C [redacted] Male, 58 y (born 1959-12-16) ID 161259-3653 ICU

D [redacted] Male, 34 y (born 1984-06-06) ID 060684-9515 ICU

E Empty bed

F Empty bed

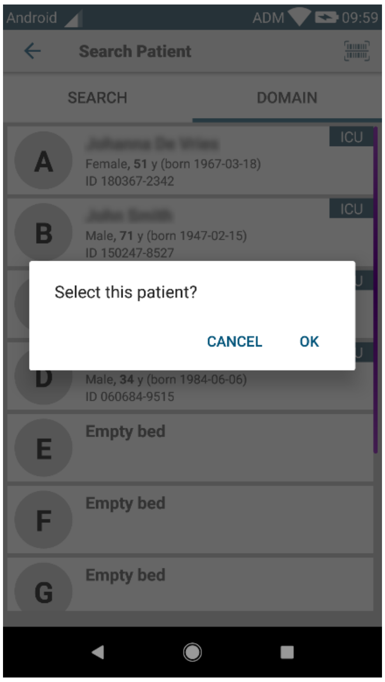
G Empty bed

H Empty bed

Fig 40

In Fig 40 all the patients are listed, without regard to their domain. The label on the top right corner of each tile highlights the domain of the patients (Fig 40 **A**).
One single patient can be selected by touching the tile corresponding to his/her bed. Just for example:

- ➢ Touch the tile indicated in Fig 40 **B**. User confirmation is required (Fig 41).



A [redacted] ICU
Female, 51 y (born 1967-03-18)
ID 180367-2342

B [redacted] ICU
Male, 71 y (born 1947-02-15)
ID 150247-8527

Select this patient?

CANCEL OK

D
Male, 34 y (born 1984-06-06)
ID 060684-9515

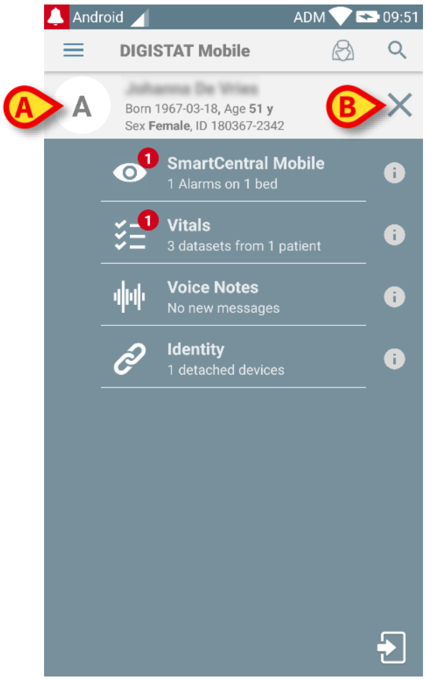
E Empty bed

F Empty bed

G Empty bed

Fig 41

- ➢ Touch **Ok** to confirm. After confirmation, the following screen is displayed.



A [redacted]
Born 1967-03-18, Age 51 y
Sex Female, ID 180367-2342

SmartCentral Mobile
1 Alarms on 1 bed

Vitals
3 datasets from 1 patient

Voice Notes
No new messages

Identity
1 detached devices

Fig 42

Patient data are on top of the page (Fig 42 **A**). All the data in all the DIGISTAT® Mobile modules are now filtered by patient (i.e. all and only the selected patient alarms/notifications are displayed).

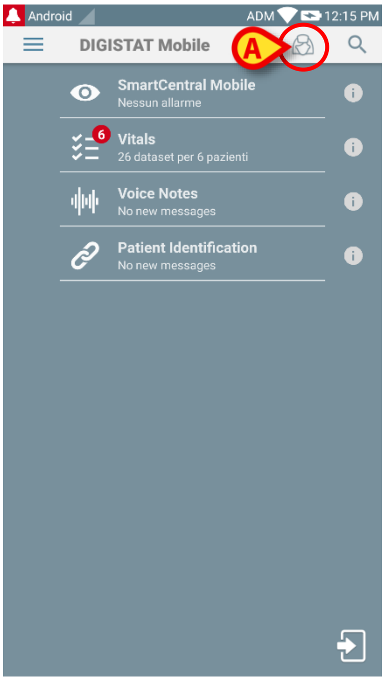
- ➢ Touch the cross indicated in Fig 42 **B** to deselect the patient.

5.8 Patients Assignment Functionality

Patient's assignment makes it possible for a user to select one or more patients and create a group of patients who are under his charge. The name of this group in the DIGISTAT® Mobile application is "My Patients".

Since the user assigns himself some patients, the following notifications can be displayed on the handheld device:

a) The notifications related to the patients assigned (i.e. in the group "My patients");
b) The notifications related to the patients assigned (i.e. in the group "My patients") and those related to the patients that no one has explicitly taken in charge;
c) The notifications related to the patients assigned (i.e. in the group "My patients"), those related to the patients that no one has explicitly taken in charge and those related to other patients if the devices which had them in charge "lose" them (for any reason, low wi-fi signal for instance).



SmartCentral Mobile
Nessun allarme

Vitals
26 dataset per 6 pazienti

Voice Notes
No new messages

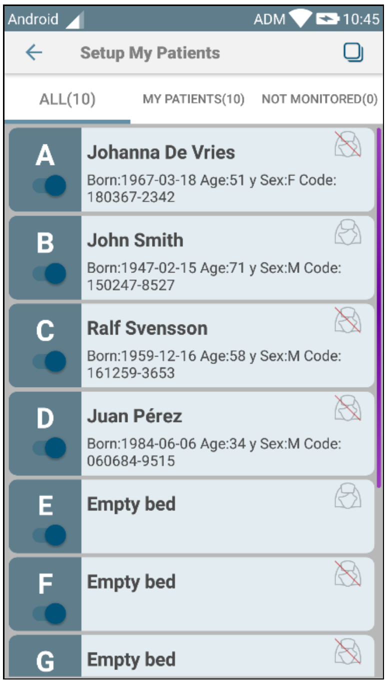
Patient Identification
No new messages

Fig 43

To select the list of patients a user assigns himself and forming "My patients" list, on DIGISTAT® Mobile Central screen,

- ➢ Touch the icon (Fig 43 **A**).

The following screen will be displayed (Fig 44 - "Setup My Patients").



Android ADM 10:45

Setup My Patients

ALL(10) MY PATIENTS(10) NOT MONITORED(0)

A Johanna De Vries
Born:1967-03-18 Age:51 y Sex:F Code: 180367-2342

B John Smith
Born:1947-02-15 Age:71 y Sex:M Code: 150247-8527

C Ralf Svensson
Born:1959-12-16 Age:58 y Sex:M Code: 161259-3653

D Juan Pérez
Born:1984-06-06 Age:34 y Sex:M Code: 060684-9515

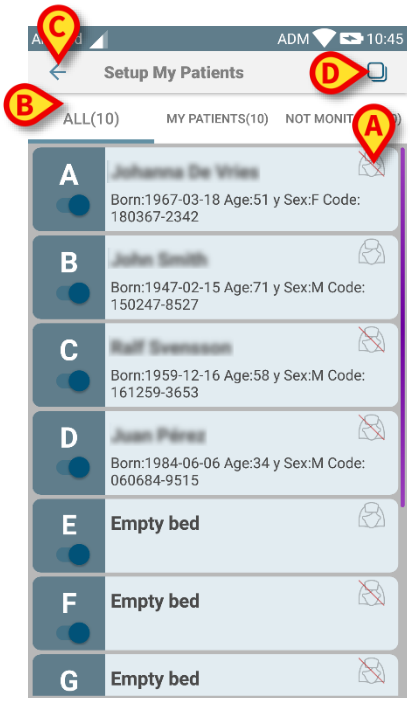
E Empty bed

F Empty bed

G Empty bed

Fig 44

A patient can be selected/deselected by touching the corresponding “tile”. Each tile corresponds to a bed. In addition, the user can select or deselect all the patients by checking the box on the top right corner (Fig 45 **D**).



Android ADM 10:45

Setup My Patients

ALL(10) MY PATIENTS(10) NOT MONIT

A
Born:1967-03-18 Age:51 y Sex:F Code: 180367-2342

B
Born:1947-02-15 Age:71 y Sex:M Code: 150247-8527

C
Born:1959-12-16 Age:58 y Sex:M Code: 161259-3653

D
Born:1984-06-06 Age:34 y Sex:M Code: 060684-9515

E Empty bed

F Empty bed

G Empty bed

Fig 45

The icons on the right of the patient names (Fig 45 **A**) have the following meanings:

- Patient is part of “My patients” of another user. It is still possible to select the patient. If two users select the same patient, the patient will be grouped under “My patients” for both users.

- Patient is not monitored. I.e. another user has him/her in charge, but at the moment, due (for example) to wi-fi connection failure, no one is monitoring him/her.
No icon means that no one has the patient in their “My patients” list, so the patient is not monitored.

The filters indicated in Fig 45 **B** make it possible to display:

- All patients;
- Only the assigned patients;
- Only the patients that are not monitored.

The ← icon indicated in Fig 45 **C** makes it possible to go back to “My Patients” list screen.

5.9 Patient selection/assignment, modules and domain

In the present document the phrase "patient selection/assignment" was used to generically refer to the operations in which a patient is selected in order to perform some operations on him within the DIGISTAT® Mobile environment. Nonetheless, for some of the modules detailed below it would be preferable to talk about "bed selection/assignment".

The main differences are detailed as follows:

- An application can operate within the domain or without the domain;
    - The Smart Central, Vitals and Voice Notes module operate within the domain. This implies that they can select beds or patients within the same domain of the user;
    - The Identity module operates without the domain. This means that Identy can establish an association patient/device even for patients outside the user domain;
- An applications operating in the domain can handle beds or patients;
    - The Smart Central module handles a bed selection (because it could be important to track data from devices coming from a bed occupied by a patient not yet identified). This implies that Smart Central can select or assign empty beds;
    - The Vitals and Voice Notes modules handle a patient selection (because it is supposed that planned parameter acquisition is performed on patients yet admitted and identified). This implies that Vitals and Voice Notes cannot select an empty bed.

6. DIGISTAT® Smart Central Mobile

6.1 Introduction

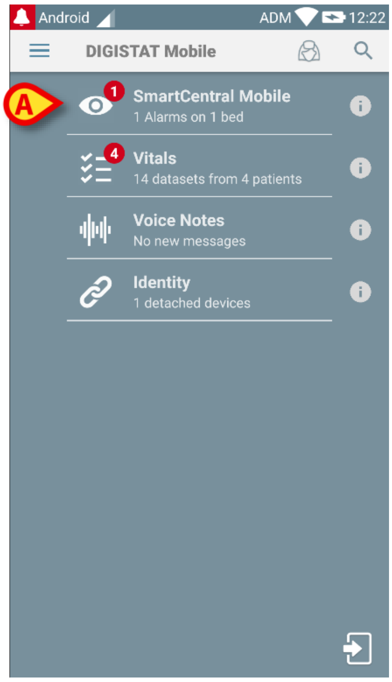
Digistat® Smart Central Mobile supports alarm management by providing contextual information from multiple sources and presenting it to the staff in a clear and concise way.

! The Product acquires the information generated by the primary medical devices and display them. Therefore, the Product always reports what the primary medical devices communicate. The assignment of alarm priorities is decided according on the primary medical device. On Digistat Smart Central it is possible to decide the order of the medical devices, for every bed, in accordance to the customer preference: per device type, model / manufacturer. The ordering of alarms is setup in Smart Central during deployment of the product according to the user request/preference. The color of every bed card is always the color of the highest priority alarm between all alarms occurring on that bed.

6.2 Application start-up

To start the Smart Central Mobile application

➢ Touch the corresponding row on the handheld device screen.



SmartCentral Mobile
1 Alarms on 1 bed

Vitals
14 datasets from 4 patients

Voice Notes
No new messages

Identity
1 detached devices

Fig 46

The Smart Central screen, shown in Fig 47 or Fig 48, opens. If the row of the application is touched while an alarm condition is raised (it is present a red number on the right top of the application symbol), then the Smart Central screen will present the list of alarmed patients.

6.3 “Central” screen

The “Central” screen displays a schematic summary of the status of the medical devices connected to each bed configured in the specific handheld device.
If all the patients of the domain are assigned to the user, then the Central screen represents the patients as a set of squares (Fig 47).

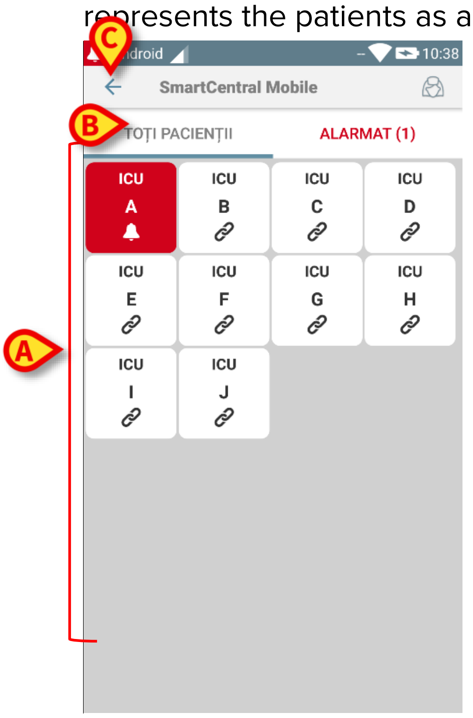
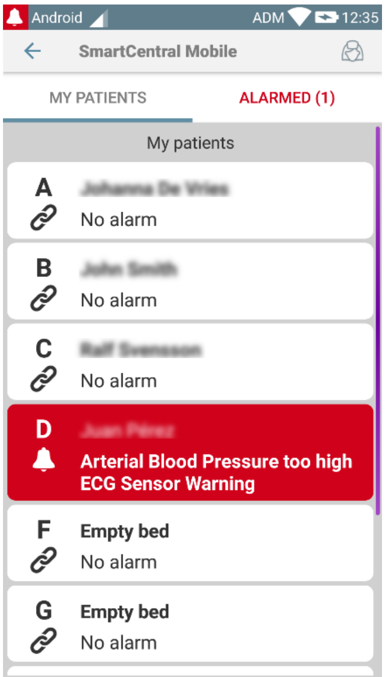


Fig 47

If NOT all the patients of the domain are assigned to the user, then the Central screen represents the patients as a set of tiles (Fig 48).



Android ADM 12:35

SmartCentral Mobile

MY PATIENTS ALARMED (1)

My patients

A [redacted]
No alarm

B [redacted]
No alarm

C [redacted]
No alarm

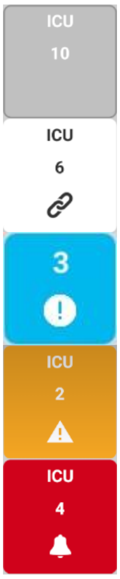
D [redacted]
Arterial Blood Pressure too high
ECG Sensor Warning

F Empty bed
No alarm

G Empty bed
No alarm

Fig 48

The squares or tiles displayed on screen represent the beds configured in the handheld device (Fig 47 **A**). The squares/tiles visible on a single screen form the “domain” of beds covered by the handheld device. The “domain” is defined by configuration.
The number or letter displayed inside the square/tile indicates the bed number or letter. On each square or tile, the status of the connected medical devices is indicated in graphic form by the background color and the related icon:



All the medical devices connected to the bed are on hold.

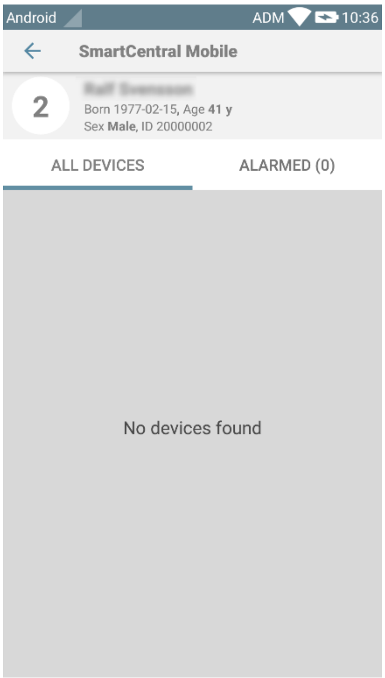
There is at least one connected medical device running.

At least one of the connected medical devices is sending a low priority alarm.

At least one of the connected medical devices is sending a medium priority alarm.

At least one of the connected medical devices is sending a high priority alarm.

The first case of the above reported scheme is the one in which no devices are sending data from the bed. In this situation, if the user touches the considered tile then the Smart Central application will display the following screen:



Android ADM 10:36

SmartCentral Mobile

2 [redacted]
Born 1977-02-15, Age **41 y**
Sex **Male**, ID 20000002

ALL DEVICES ALARMED (0)

No devices found

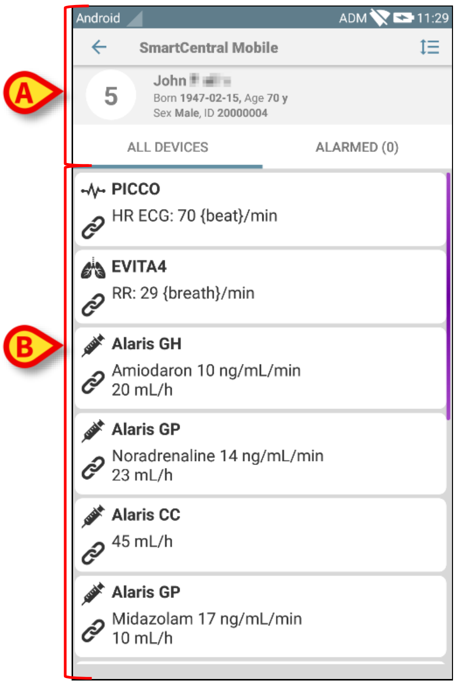
Fig 49

You can use the filters indicated in Fig 47 **B** to display either all the configured beds or only the beds sending an alarm.
It is possible to configure the Smart Central application to wake the screen if an alarm is raised to the user and the mobile device is on a flat support (a desktop, a table, etc.).

Exit
Touch the **Exit** button (Fig 47 **C**) to quit the application.

6.4 Medical devices list

Touch one of the squares on the “Central” screen to display the list of medical devices connected to the bed (Fig 50).



Android ADM 11:29

SmartCentral Mobile

5 John [redacted]
Born 1947-02-15, Age 70 y
Sex Male, ID 20000004

ALL DEVICES ALARMED (0)

PICCO
HR ECG: 70 {beat}/min

EVITA4
RR: 29 {breath}/min

Alaris GH
Amiodaron 10 ng/mL/min
20 mL/h

Alaris GP
Noradrenaline 14 ng/mL/min
23 mL/h

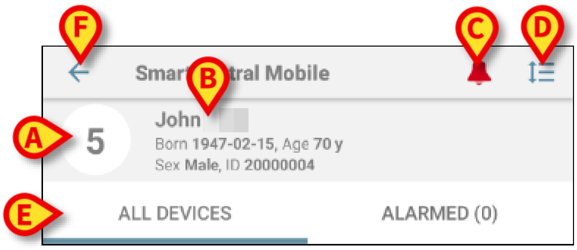
Alaris CC
45 mL/h

Alaris GP
Midazolam 17 ng/mL/min
10 mL/h

Fig 50

This screen is formed of two areas: a heading area (Fig 50 **A**) and the medical devices list (Fig 50 **B**). If an alarm conditions is present, the “Alarmed” label is colored in red.

6.4.1 Heading



SmartCentral Mobile

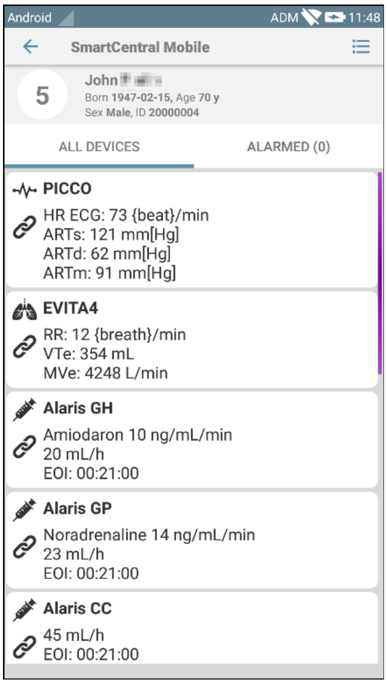
5 John [redacted]
Born 1947-02-15, Age 70 y
Sex Male, ID 20000004

ALL DEVICES ALARMED (0)

Fig 51

In the heading area (Fig 51) the following information and tools are available:

- Bed number (Fig 51 **A**).
- Patient data (Fig 51 **B**).
- The red bell icon (Fig 51 **C**) indicates that there is at least one medical device alarmed on one of the other beds (those not currently displayed). If the red bell icon is touched, then the Smart Central screen will present the list of alarmed patients.
- Use the icon indicated in Fig 51 **D** to enlarge the device-areas and display more information for each connected medical device (Fig 52). The type of information displayed depends on the configuration and the specific device.



Android ADM 11:48

SmartCentral Mobile

5 John [redacted]
Born 1947-02-15, Age 70 y
Sex Male, ID 20000004

ALL DEVICES ALARMED (0)

PICCO
HR ECG: 73 {beat}/min
ARTs: 121 mm[Hg]
ARTd: 62 mm[Hg]
ARTm: 91 mm[Hg]

EVITA4
RR: 12 {breath}/min
VTe: 354 mL
MVe: 4248 L/min

Alaris GH
Amiodaron 10 ng/mL/min
20 mL/h
EOI: 00:21:00

Alaris GP
Noradrenaline 14 ng/mL/min
23 mL/h
EOI: 00:21:00

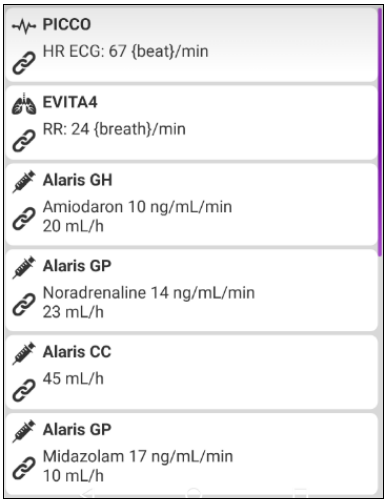
Alaris CC
45 mL/h
EOI: 00:21:00

Fig 52

- ➢ Touch the icon (Fig 51 **D**) again to go back to compact display mode.
- ➢ Use the filters indicated in Fig 51 **E** to display either all the connected medical devices or only the ones providing notifications.
- ➢ Use the back-arrow button (Fig 51 **F**) to go back to the “Central” screen.

6.4.2 Devices list

On the lower part of the “Bed” screen the individual medical devices are represented as shown in Fig 53:



PICCO
HR ECG: 67 {beat}/min

EVITA4
RR: 24 {breath}/min

Alaris GH
Amiodaron 10 ng/mL/min
20 mL/h

Alaris GP
Noradrenaline 14 ng/mL/min
23 mL/h

Alaris CC
45 mL/h

Alaris GP
Midazolam 17 ng/mL/min
10 mL/h

Fig 53

Each medical device is represented within a “card”. Each “card” displays the following information:

- An icon indicating the medical device type. The list of possible icons changes according to the healthcare organization needs. Here are some common examples:

  Infusion Pump

  Respirator

  Cardiac Output Measurement Machine

- An icon indicating the medical device status. These are:

  On hold

  Running

  Sending a low priority alarm notification

  Sending a medium priority alarm notification

  Sending a high priority alarm notification

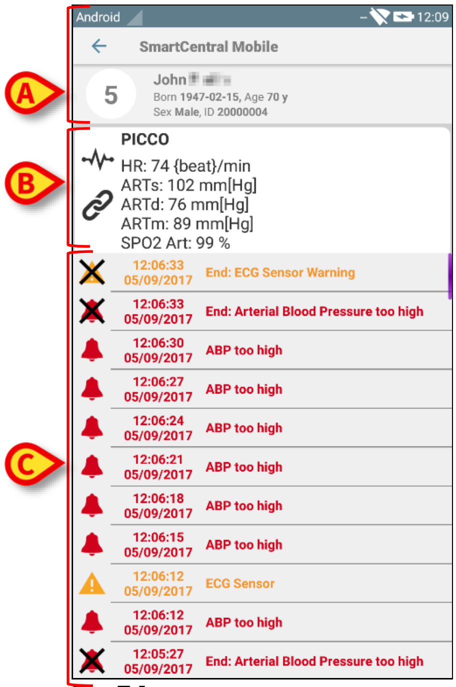
The background color of the “card” also indicates the medical device status: grey (on hold); white (running); cyan (low priority alarm); yellow (medium priority alarm); red (high priority alarm).

For each medical device, some basic information is displayed inside the “card”. The type of information depends on configuration.

In case of alarm the “card” displays the alarm message.

6.5 Alarms history

Each “card” can be touched to access the list of all the alarms provided by the medical device (Fig 54).



Android 12:09

SmartCentral Mobile

5 John [redacted]
Born 1947-02-15, Age 70 y
Sex Male, ID 20000004

PICCO
HR: 74 {beat}/min
ARTs: 102 mm[Hg]
ARTd: 76 mm[Hg]
ARTm: 89 mm[Hg]
SPO2 Art: 99 %

✗	12:06:33 05/09/2017	End: ECG Sensor Warning
✗	12:06:33 05/09/2017	End: Arterial Blood Pressure too high
🔔	12:06:30 05/09/2017	ABP too high
🔔	12:06:27 05/09/2017	ABP too high
🔔	12:06:24 05/09/2017	ABP too high
🔔	12:06:21 05/09/2017	ABP too high
🔔	12:06:18 05/09/2017	ABP too high
🔔	12:06:15 05/09/2017	ABP too high
⚠	12:06:12 05/09/2017	ECG Sensor
🔔	12:06:12 05/09/2017	ABP too high
✗	12:05:27 05/09/2017	End: Arterial Blood Pressure too high

Fig 54

This screen is formed of three areas.

Patient data (Fig 54 **A**).
Medical device current data. The data displayed on this “card”, again depend on the device type and configuration (Fig 54 **B**).
Notification history. Displaying, in chronological order, all the alarms occurred on the device. For each alarm, a short description and the time of occurrence are provided (Fig 54 **C**). For each alarm are displayed the beginning time and end time (black cross on the icon ✗).

7. DIGISTAT® "Vitals"

7.1 Introduction

The "Vitals" App is intended to permit data entry and display for a variety of clinical workflows, procedures and protocols within the healthcare services domain.
Examples:

- Patient vital signs data collection for normal wards.
- Patient data collection for clinical protocols associated to specific diseases, treatments or prevention of diseases.
- Generation of reminders for periodic data collection or patient examination and documentation of the activity performed and provided services.
- Documentation of patient conditions also by means of pictures and audio recordings.

7.2 Application start-up

To start the "Vitals" application

➢ Touch the corresponding row on the handheld device screen (Fig 55).

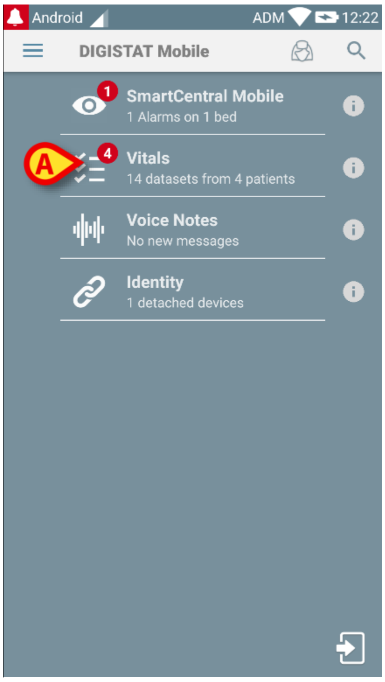
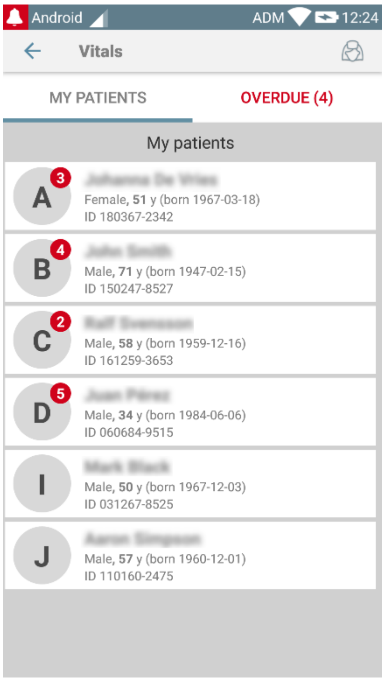


Fig 55

The "Vitals" screen, shown in Fig 56, will open.



My patients

A 3 [redacted]
Female, **51** y (born 1967-03-18)
ID 180367-2342

B 4 [redacted]
Male, **71** y (born 1947-02-15)
ID 150247-8527

C 2 [redacted]
Male, **58** y (born 1959-12-16)
ID 161259-3653

D 5 [redacted]
Male, **34** y (born 1984-06-06)
ID 060684-9515

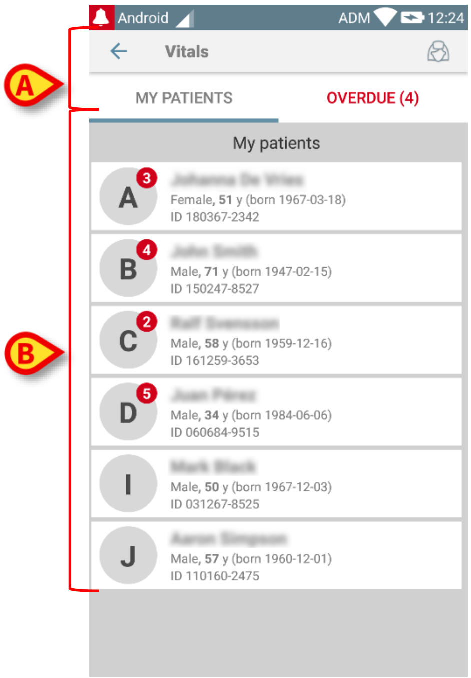
I [redacted]
Male, **50** y (born 1967-12-03)
ID 031267-8525

J [redacted]
Male, **57** y (born 1960-12-01)
ID 110160-2475

Fig 56

7.3 Patients list

The “Vitals” patient list screen (Fig 57) displays the list of beds configured on the handheld device (namely, the device “domain”).
The domain of a specific handheld device is defined by configuration. In case there is no patient on one of the configured beds, then the bed is not displayed.



My patients

A 3 [redacted]
Female, **51** y (born 1967-03-18)
ID 180367-2342

B 4 [redacted]
Male, **71** y (born 1947-02-15)
ID 150247-8527

C 2 [redacted]
Male, **58** y (born 1959-12-16)
ID 161259-3653

D 5 [redacted]
Male, **34** y (born 1984-06-06)
ID 060684-9515

I [redacted]
Male, **50** y (born 1967-12-03)
ID 031267-8525

J [redacted]
Male, **57** y (born 1960-12-01)
ID 110160-2475

Fig 57

The patient list screen is formed of a heading (Fig 57 **A**) and the patients list (Fig 57 **B**).

7.3.1 Patient list heading

Fig 58 shows the heading of the patient list screen.

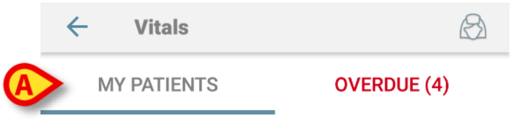


Fig 58

The filter indicated in Fig 58 **A** makes it possible to display either all the patients configured on the handheld device domain (**All Patients**) or only the patients for which there are notifications overdue (**Overdue**).

7.3.2 List of beds

Each bed is represented by a tile (Fig 59).

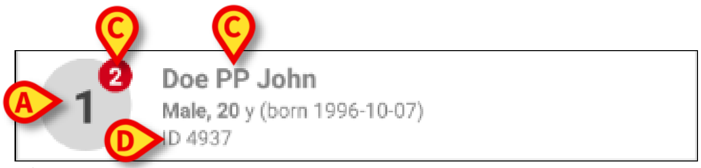


Fig 59

In the tile, the following information is displayed:

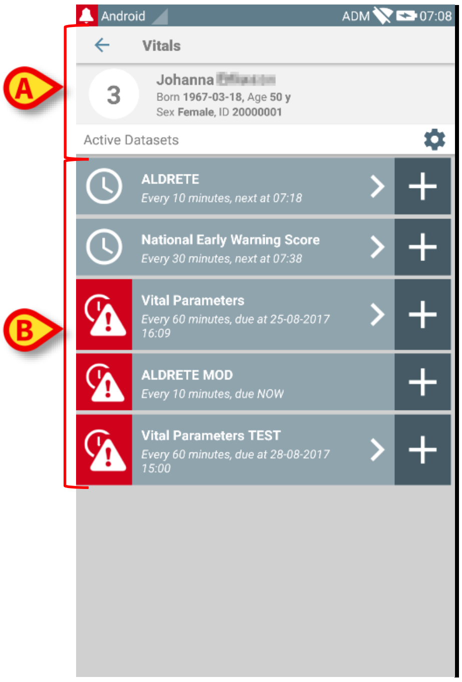
- bed number (Fig 59 **A**);
- number of notifications overdue (if any - Fig 59 **B**);
- name of patient on that bed (Fig 59 **C**);
- patient data (if available: sex, age, date of birth, patient ID - Fig 59 **D**).

➢ Touch one tile to access the list of datasets enabled for the corresponding patient (Fig 60).

The term “Dataset” refers to a structured set of data, considered as a whole. It can be, for instance, a score calculation, a set of vital parameters etc.

7.4 Datasets list

The datasets list screen is formed of two areas: a heading area (Fig 60 **A**) and the list of datasets (Fig 60 **B**).



Vitals

3 Johanna [redacted]
Born 1967-03-18, Age 50 y
Sex Female, ID 20000001

Active Datasets

ALDRETE
Every 10 minutes, next at 07:18

National Early Warning Score
Every 30 minutes, next at 07:38

Vital Parameters
Every 60 minutes, due at 25-08-2017 16:09

ALDRETE MOD
Every 10 minutes, due NOW

Vital Parameters TEST
Every 60 minutes, due at 28-08-2017 15:00

Fig 60

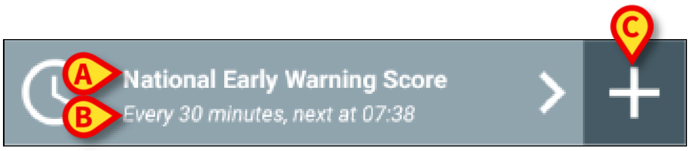
The heading area displays the following information:

- bed number;
- name of patient on that bed;
- patient data (if available: sex, age, date of birth, patient ID).

The datasets are displayed in tiles below the heading area. Each tile represents a dataset.

The information displayed inside the tiles depends on the kind of dataset and the way the dataset is configured. See paragraph 7.4.5 for the dataset configuration functionalities.

Fig 61 shows an example.



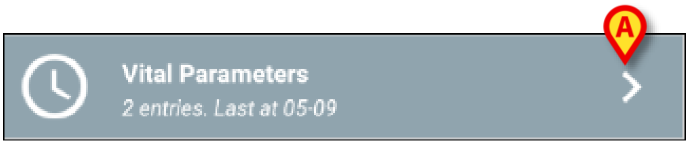
National Early Warning Score
Every 30 minutes, next at 07:38

Fig 61

The dataset name is displayed inside the tile (“National Early Warning Score” - Fig 61 **A**).
Below the dataset name, information is displayed relating the data acquisition modalities (i.e. when the dataset shall be acquired, when is the next acquisition due etc. - all these data depend on how the dataset is configured - Fig 61 **B**).

The + button (Fig 61 **C**) makes it possible to insert new data (see paragraph 7.4.1).

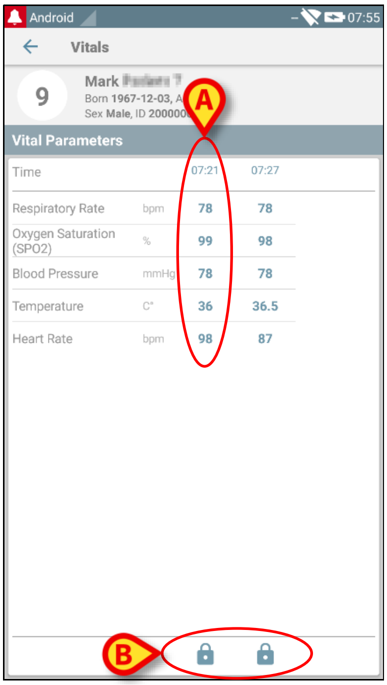
If the + button is not present on the tile it means that the dataset is not enabled (see paragraph 7.4.5 for more information). The tile is still displayed because past data exists for that dataset, which can be still viewed. See for instance Fig 62.



Vital Parameters
2 entries. Last at 05-09

Fig 62

The arrow (Fig 62 **A**) makes it possible to display the past data. See for example Fig 63.



Android 07:55

Vitals

9 Mark [redacted]
Born 1967-12-03, A
Sex Male, ID 200000

Vital Parameters

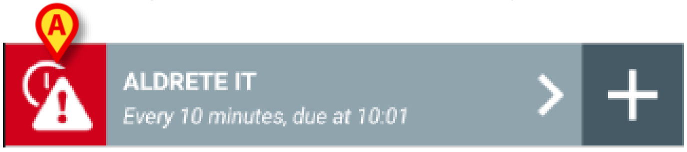
Time		07:21	07:27
Respiratory Rate	bpm	78	78
Oxygen Saturation (SPO2)	%	99	98
Blood Pressure	mmHg	78	78
Temperature	C°	36	36.5
Heart Rate	bpm	98	87

Fig 63

For each entry (i.e. a set of values), date and time are displayed on top. The recorded values are displayed below. See for instance the column indicated in Fig 63 **A**.

The “lock” icon indicated in Fig 63 **B** means that the corresponding score cannot be edited. Otherwise a “pen” icon is displayed (see for instance Fig 70).

The datasets can be configured to provide a notification at scheduled times, as a reminder, when they should be acquired. See for instance Fig 64. The Aldrete score is here configured to be acquired every 10 minutes.



ALDRETE IT
Every 10 minutes, due at 10:01

Fig 64

If the dataset is not acquired on time, the system displays a notification, meaning that an action was due at a certain time but the action was not performed. The icon indicated in Fig 64 **A** is then displayed.
The handheld device in this case provides a specific sound/vibration. The notification is provided on the handheld device even if Vitals is not active. Also, a visual note is displayed on screen (see paragraph 5.6).

7.4.1 How to record a new set of data

To record a new set of data

➢ Touch the + icon on the tile corresponding to the wanted dataset (Fig 65).

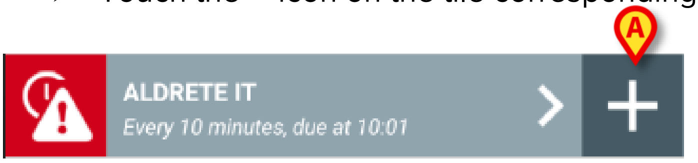


Fig 65

The data entry screen will be displayed.

NOTE: the data entry screen features depend on the kind of dataset selected. See Fig 66 for an example.

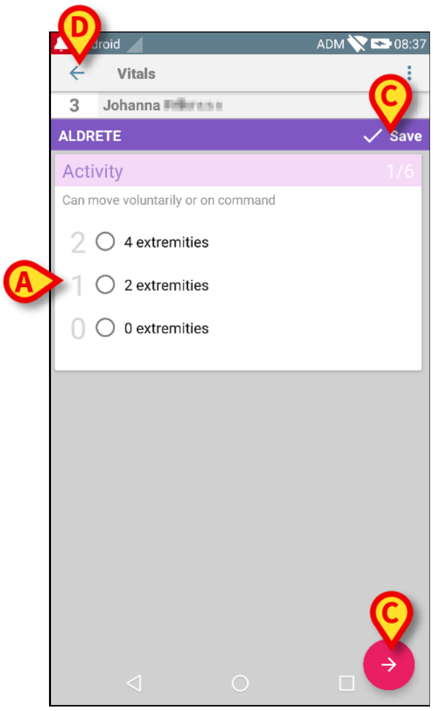


Fig 66

A score can be configured to indicate with a color code the degree of urgency/severity of the available values. The same color code will be then applied to the final result. Also, if so configured, a text indication about the therapy/treatment can be associated to a certain results range.

See Fig 67 for another example.

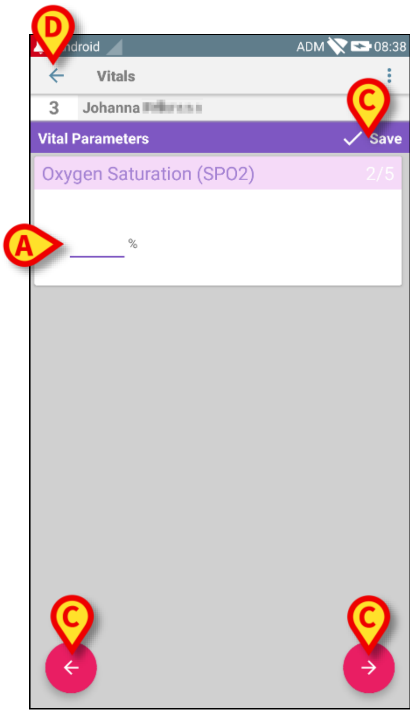


Fig 67

In general, data specification is divided in a number of different screens (one for each kind of data/question/parameter).

- ➢ Insert the required value/s on each screen (Fig 66 **A** and Fig 67 **A**).
- ➢ Move to next/previous screen using the arrows indicated in Fig 66 **B** and Fig 67 **B**.

When all the (relevant/known) values have been specified,

- ➢ Touch **Save** to save the dataset (Fig 66 **C** and Fig 67 **C**). The **Cancel** option (Fig 66 **D** and Fig 67 **D**) closes the data entry screen.

In addition to the insertion scheme above explained, it is moreover possible to configure the dataset in order to show all the requested parameter in a single page. This is ever possible with the exception of dataset accounting audio and photo as input parameters (Fig 68).

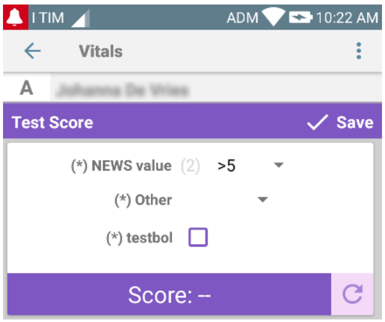
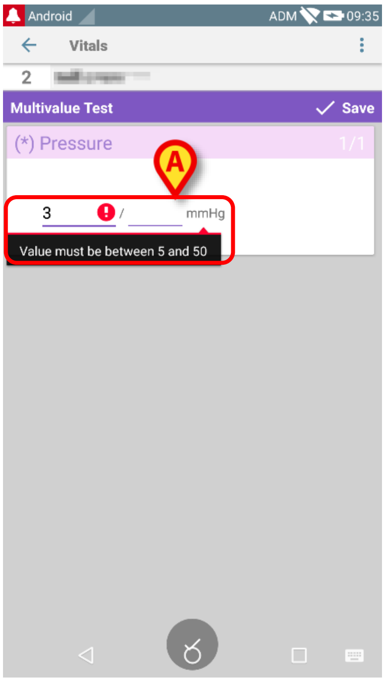


Fig 68

The system can be configured to consider as “Valid” only the values included in a determined range and to therefore not accept values outside the configured range.

If values outside the range are inserted, the system rejects them with a message informing the user about the range of acceptable values. See for instance Fig 69 **A**.



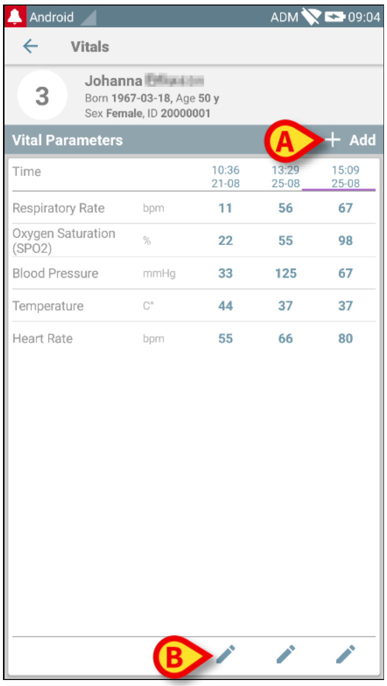
3 /

Value must be between 5 and 50

Fig 69

7.4.2 Inserted values summary

The recorded sets of values are displayed in a specific summary screen. Again, the screen features depend on the kind of dataset acquired. See Fig 70 for an example.



3 Johanna [redacted]
Born 1967-03-18, Age 50 y
Sex Female, ID 20000001

Vital Parameters

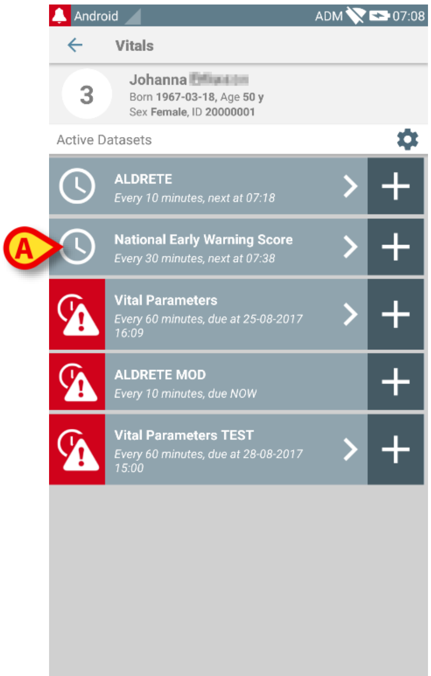
Time		10:36 21-08	13:29 25-08	15:09 25-08
Respiratory Rate	bpm	11	56	67
Oxygen Saturation (SPO2)	%	22	55	98
Blood Pressure	mmHg	33	125	67
Temperature	C°	44	37	37
Heart Rate	bpm	55	66	80

Fig 70

- ➢ On this screen, touch **Add** to add another set of data (Fig 70 **A**).
- ➢ Use the “Pen” icon to edit the data of an existing set (Fig 70 **B**).

7.4.3 How to edit an existing set of data

To edit an existing set of data, on the datasets list screen (Fig 71),



Vitals

3 Johanna [redacted]
Born 1967-03-18, Age 50 y
Sex Female, ID 20000001

Active Datasets

ALDRETE
Every 10 minutes, next at 07:18

National Early Warning Score
Every 30 minutes, next at 07:38

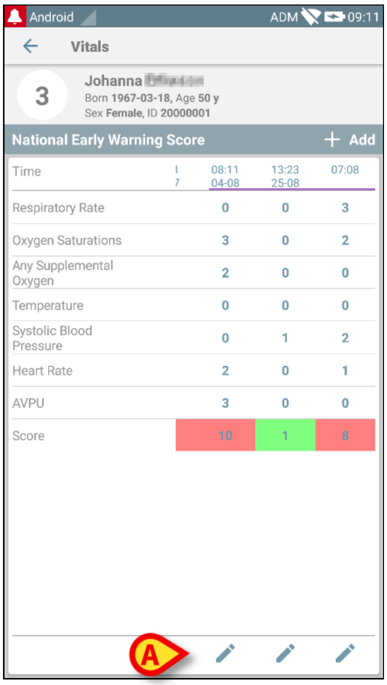
Vital Parameters
Every 60 minutes, due at 25-08-2017 16:09

ALDRETE MOD
Every 10 minutes, due NOW

Vital Parameters TEST
Every 60 minutes, due at 28-08-2017 15:00

Fig 71

- ➢ Select the relevant dataset (Fig 71 **A**, for instance). The acquired datasets summary will open (Fig 72).



Vitals

3 Johanna [redacted]
Born 1967-03-18, Age 50 y
Sex Female, ID 20000001

National Early Warning Score + Add

Time	I 7	08:11 04-08	13:23 25-08	07:08
Respiratory Rate		0	0	3
Oxygen Saturations		3	0	2
Any Supplemental Oxygen		2	0	0
Temperature		0	0	0
Systolic Blood Pressure		0	1	2
Heart Rate		2	0	1
AVPU		3	0	0
Score		10	1	8

Fig 72

- ➢ Touch the “pen” icon corresponding to the set to be edited (Fig 72 **A**)

The data entry screen will open (Fig 73).

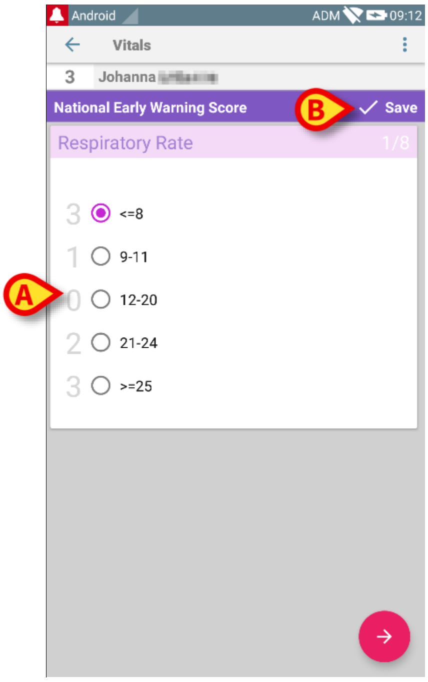


Fig 73

- ➢ Edit data (Fig 73 **A**).
- ➢ Touch **Save** (Fig 73 **B**).

The set is this way edited.

7.4.4 Pictures and audio acquisition

The “Vitals” module makes it possible to acquire audio recordings and pictures. This functionality can be configured both as a specific, independent dataset, and as a part of an existing “textual” dataset. In the latter case the functionality makes it possible to add an audio/visual commentary to the recorded values.

To start the audio/image acquisition, on the datasets list

- ➢ Touch the “**+**” button placed on the right of the dedicated dataset (Fig 74 **A**).

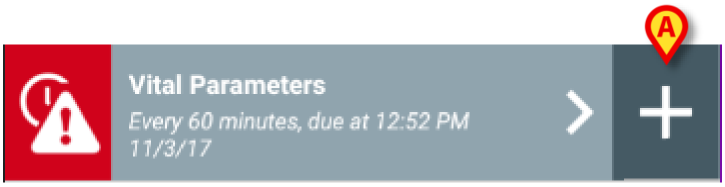


Fig 74

The following screen will open, making it possible to record an audio file (Fig 75).

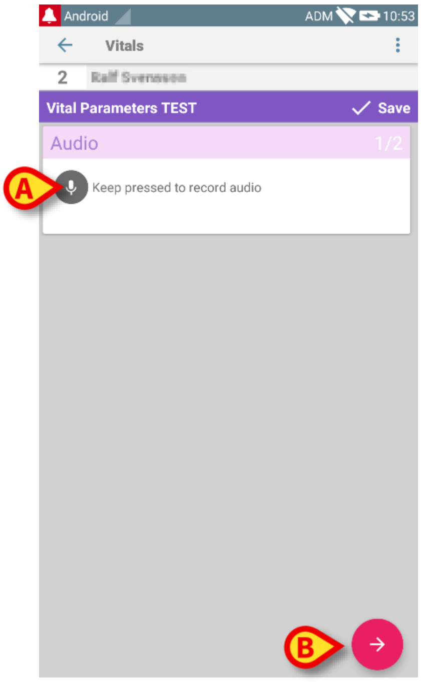


Fig 75

To record,

- Keep pressed the button indicated in Fig 75 **A**.

The button will turn red while recording. Recording ends when the button is released. After recording the audio acquisition page is displayed (Fig 76). The icon indicated in Fig 76 **A** represents the recorded file.

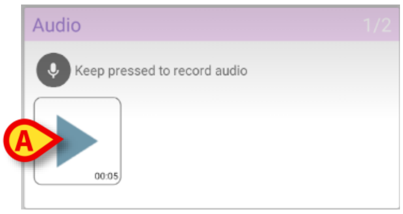


Fig 76

Multiple recordings are possible for a single dataset acquisition (Fig 77 **A**).

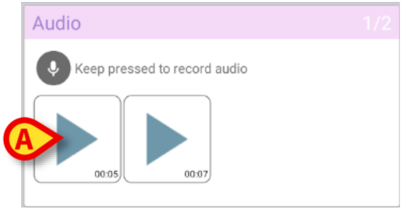


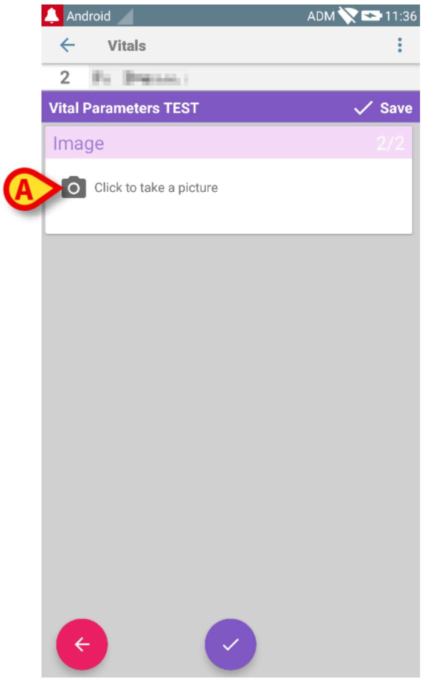
Fig 77

- Touch the icon to listen to the audio file.

For pictures acquisition, go to the following screen, i.e.

- Touch the → icon on the lower-right corner of the screen (Fig 75 **B**).

The following screen will open (Fig 78)


Android ADM 11:36

Vitals

2 [redacted]

Vital Parameters TEST ✓ Save

Image 2/2

Click to take a picture

Fig 78

- Touch the icon indicated in Fig 78 **A** to activate the camera (Fig 79).

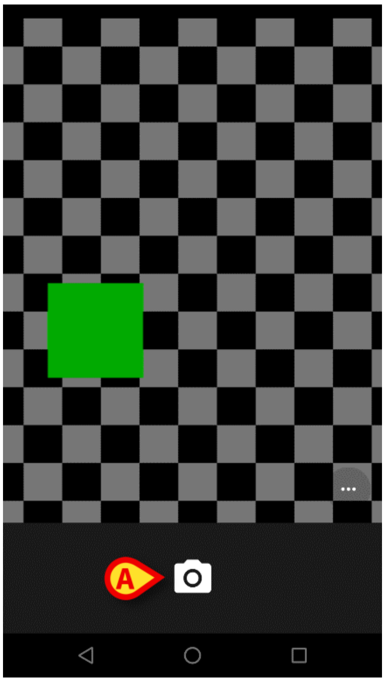


Fig 79

- Touch the 📷 icon to take the picture (Fig 79 **A**). A preview is displayed on screen (Fig 80).

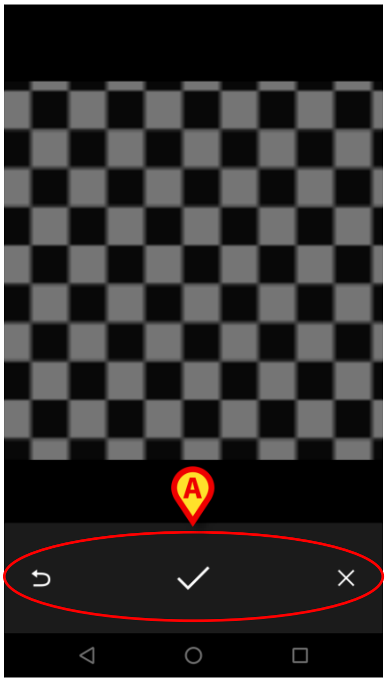


Fig 80

- Use the buttons indicated in Fig 80 **A** to:
  1. go back to the picture acquisition mode (Fig 79);
  2. keep the picture and go back to the photo acquisition page (Fig 78);
  3. discard the picture and go back to the photo acquisition page (Fig 78).

Once a picture is saved, a thumbnail is displayed on the photo acquisition page (Fig 81).

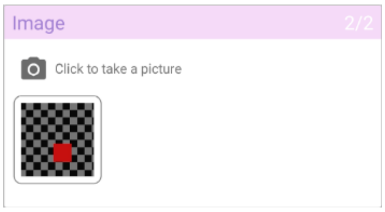


Fig 81

- Touch the thumbnail to display the picture again.

Multiple pictures can be acquired for the same dataset.

After audio and/or picture acquisition, to save the acquired data, on the photo acquisition page (Fig 82),

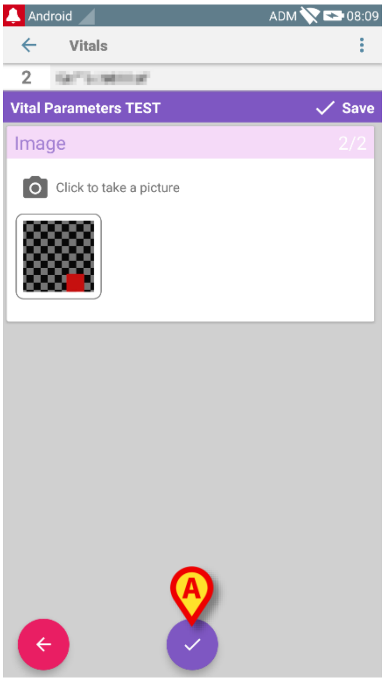
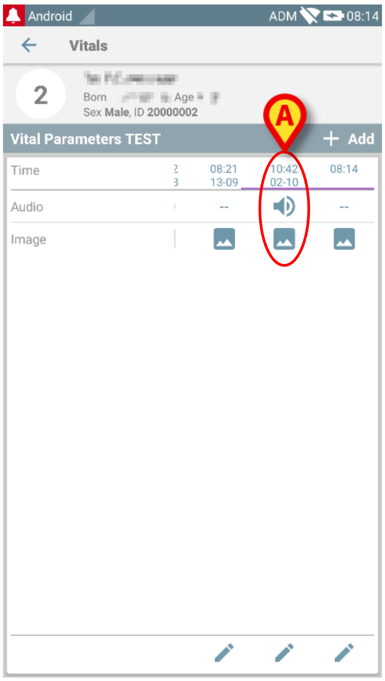


Fig 82

➢ Click the ✓ icon (Fig 82 **A**).

A summary screen is then displayed, listing all the acquired datasets (Fig 83).



Time		08:21 13-09	10:42 02-10	08:14
Audio		--	🔊	--
Image		🖼	🖼	🖼

Fig 83

On this page, each column corresponds to a dataset (Fig 83 **A**). For each dataset the following information is provided:

- Date/time of acquisition.
- There is at least an audio recorded - 🔊 icon.
- There is at least a picture saved - 🖼 icon.

7.4.5 How to use OCR functionality

! The OCR functionality is not supported on Myco1 devices and in general on devices with Android version 4.4.2 and lower; it is supported on the Myco2 devices and in general on Myco devices with firmware version 10.1 and higher, or in general on Android devices with version 5.1 and higher.

The OCR (Optical Character Recognition) functionality is useful since there is the necessity to read and record data from the General Electric V100 monitor.

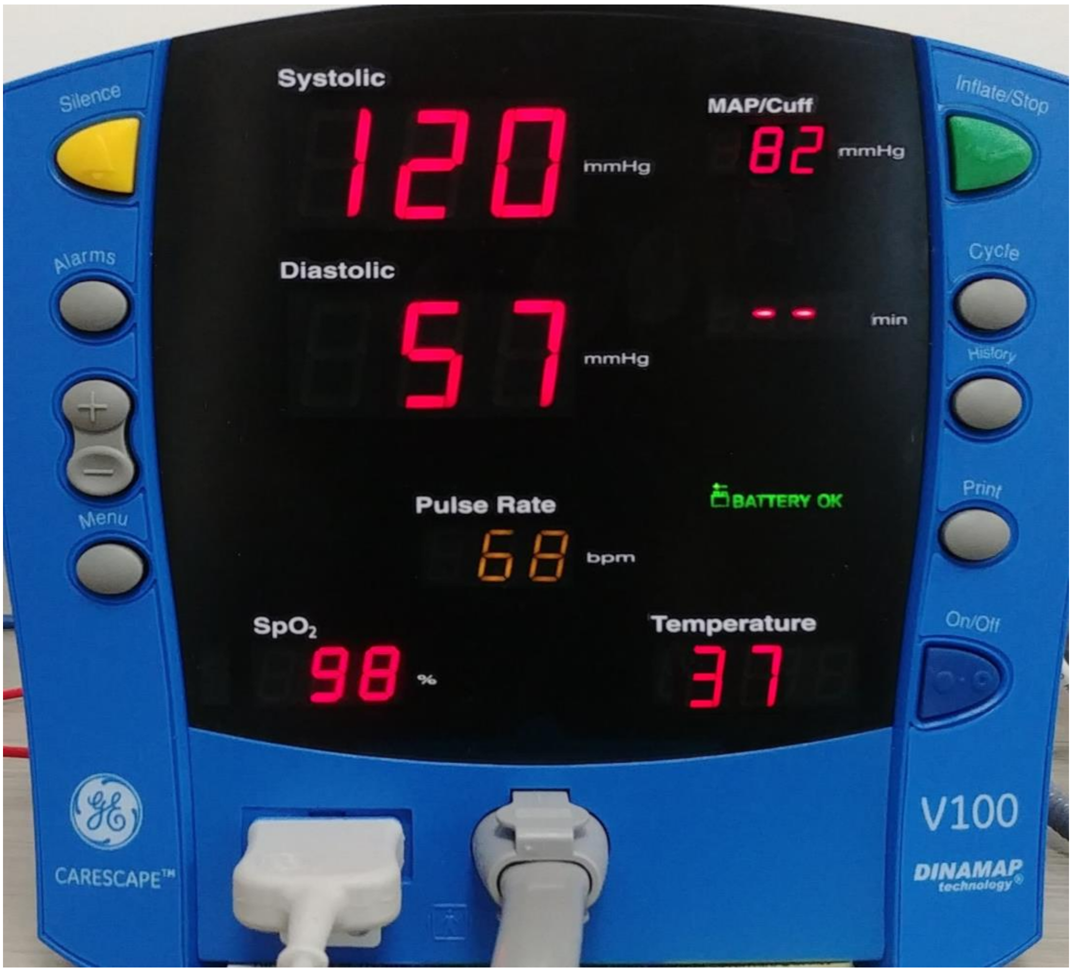


Fig 84 - General Electric V100 monitor

! At the present stage of development only the General Electric V100 model of monitor is supported for the OCR functionality.

Just as explained in the Paragraph 7.4.1, to record a new set of data based on the OCR functionality

- ➢ Touch the + icon on the tile corresponding to the wanted dataset (Fig 85 **A**)

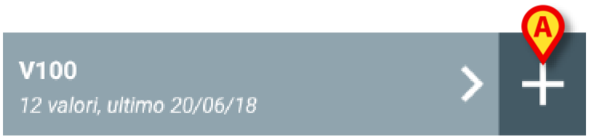
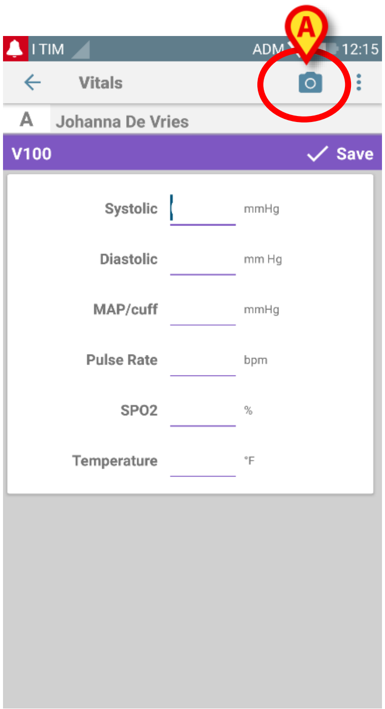


Fig 85

The data entry screen will be displayed (Fig 86).



Systolic		mmHg
Diastolic		mm Hg
MAP/cuff		mmHg
Pulse Rate		bpm
SPO2		%
Temperature		°F

Fig 86

- ➢ Touch the 📷 icon on the top of the screen (Fig 86 **A**).
  The screen for the image acquisition will appear. Since the device is not almost perfectly in vertical position and in front of the monitor, a message suggest the user to correct its grip (Fig 87 **A**).

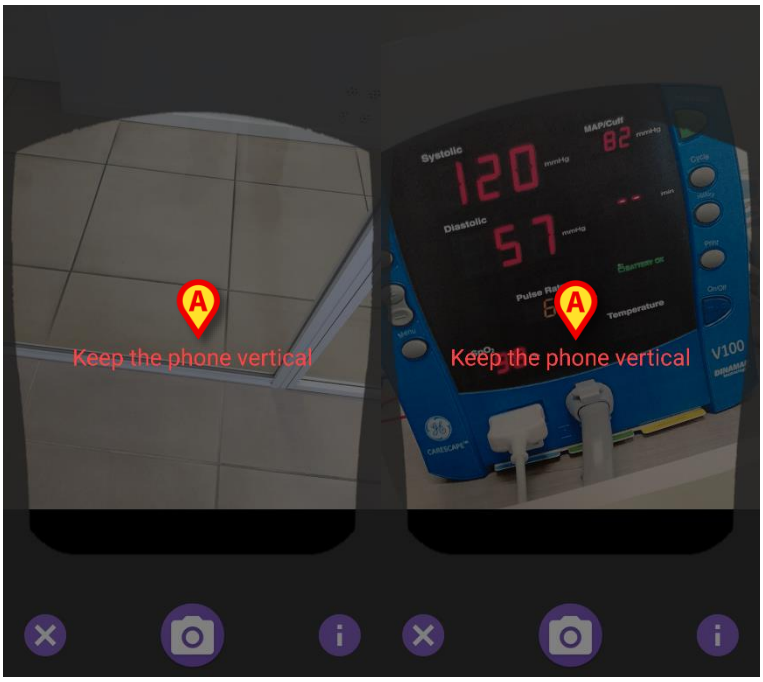


Fig 87

- ➢ Touch the ◎ icon to acquire the photo in the current position (Fig 88 **A**) or the ⊗ icon to abort the picture (Fig 88 **B**).

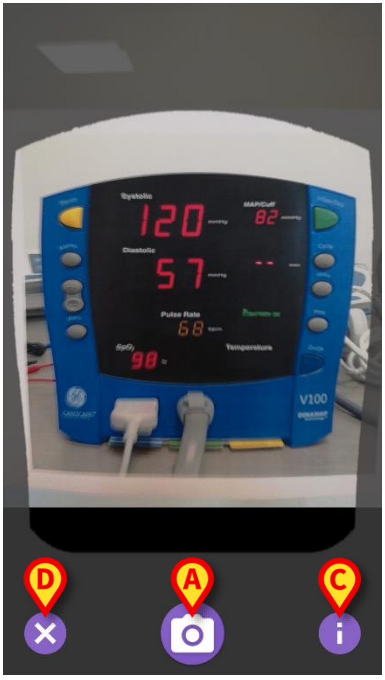
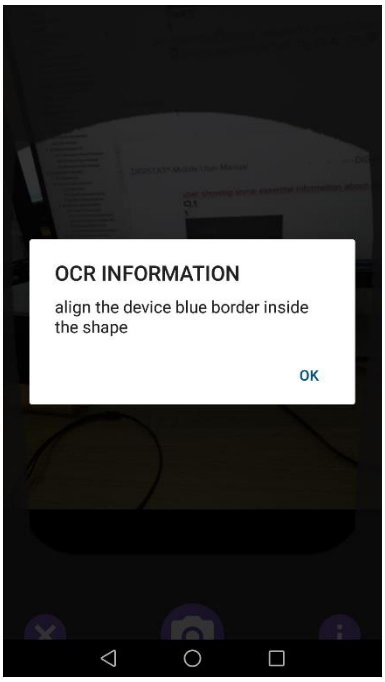


Fig 88

- ➢ Touch the ⓘ button to read a help for the user showing some essential information about the OCR functionality (Fig 88 **C**).
  The following window is displayed (Fig 89):

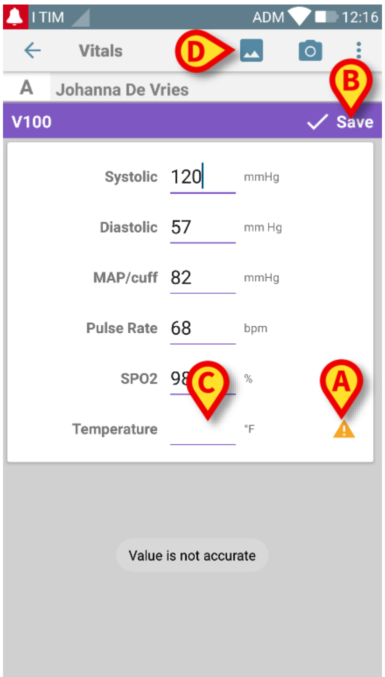


OCR INFORMATION

align the device blue border inside the shape

Fig 89

Once the photo is taken, it is processed by the OCR and the result is used to fulfill the fields of the screen Fig 86 with the data read from the device shown in Fig 84. The following window appears (Fig 90):



Systolic 120 mmHg

Diastolic 57 mm Hg

MAP/cuff 82 mmHg

Pulse Rate 68 bpm

SPO2 98 %

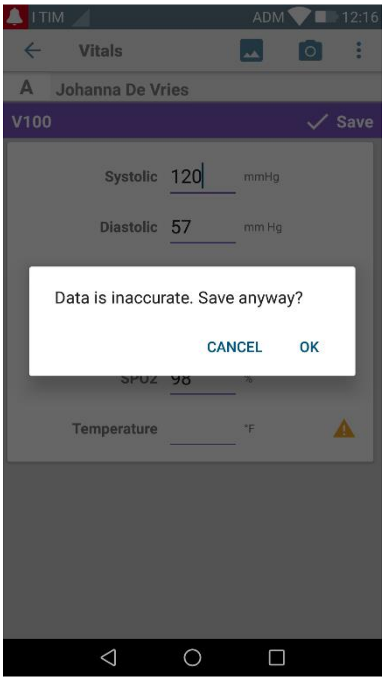
Temperature °F

Value is not accurate

Fig 90

If one of the values output from the OCR is outside the valid range, the ⚠ icon is shown close to the parameter itself (Fig 90 **A)**. This happens because the OCR was not able to recognize the values displayed by the V100 monitor or because the monitor itself did not display any value.
The button in Fig 90 **D** shows the acquired photo.

- Touch the **Save** button in the top right corner (Fig 90 **B**). If not all the values are considered in the acceptance range (i.e. there is the ⚠ icon) then the Vitals module asks for confirmation from the user (Fig 91):

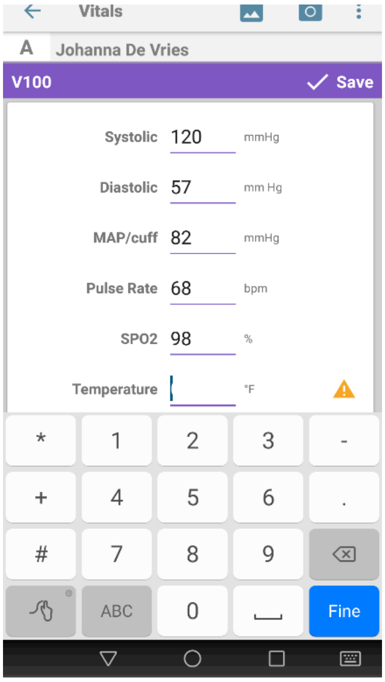


Data is inaccurate. Save anyway?

CANCEL OK

Fig 91

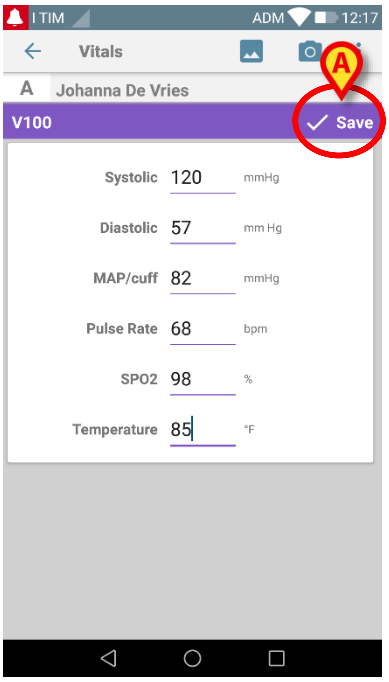
- Press **OK** to save anyway, or **CANCEL** to insert manually the missing value.
- Touch the space where it is expected to insert the missing value (Fig 90 **C**). Because a numeric value is expected, it is shown a numeric keyboard to provide the desired value (Fig 92):



Systolic	120	mmHg
Diastolic	57	mm Hg
MAP/cuff	82	mmHg
Pulse Rate	68	bpm
SPO2	98	%
Temperature		°F

Fig 92

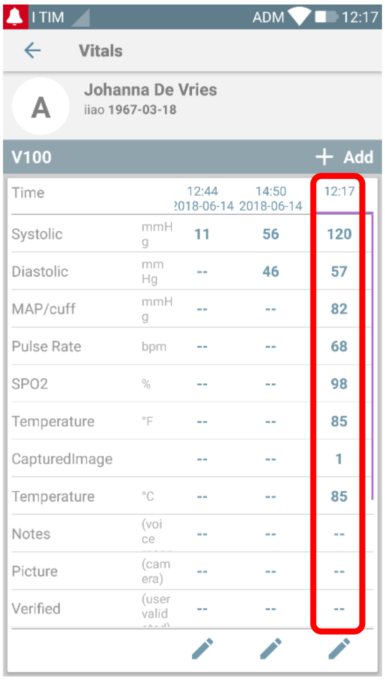
Once the desired value is inserted, the following screen will appear (Fig 93):



Systolic	120	mmHg
Diastolic	57	mm Hg
MAP/cuff	82	mmHg
Pulse Rate	68	bpm
SPO2	98	%
Temperature	85	°F

Fig 93

➢ Touch the **Save** button in the top right corner (Fig 93 **A**).
The following window will appear, resuming the last acquisitions of the considered item (Fig 94):



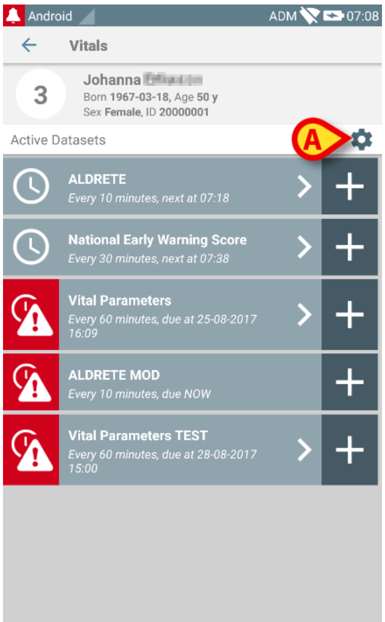
Time		12:44 2018-06-14	14:50 2018-06-14	12:17
Systolic	mmHg	11	56	120
Diastolic	mm Hg	--	46	57
MAP/cuff	mmHg	--	--	82
Pulse Rate	bpm	--	--	68
SPO2	%	--	--	98
Temperature	°F	--	--	85
CapturedImage		--	--	1
Temperature	°C	--	--	85
Notes	(voice	--	--	--
Picture	(camera)	--	--	--
Verified	(user valid	--	--	--

Fig 94

7.5 Enabling and configuring the existing datasets

NOTE: the functionalities described in this paragraph are reserved to “super users” or system administrators and require therefore a specific permission level.
To access the dataset configuration options, after patient selection, on the datasets list screen (Fig 95),

- Touch the ⚙ icon (Fig 95 **A**).


Android ADM 07:08

Vitals

3 Johanna [redacted]
Born 1967-03-18, Age 50 y
Sex Female, ID 20000001

Active Datasets

ALDRETE
Every 10 minutes, next at 07:18

National Early Warning Score
Every 30 minutes, next at 07:38

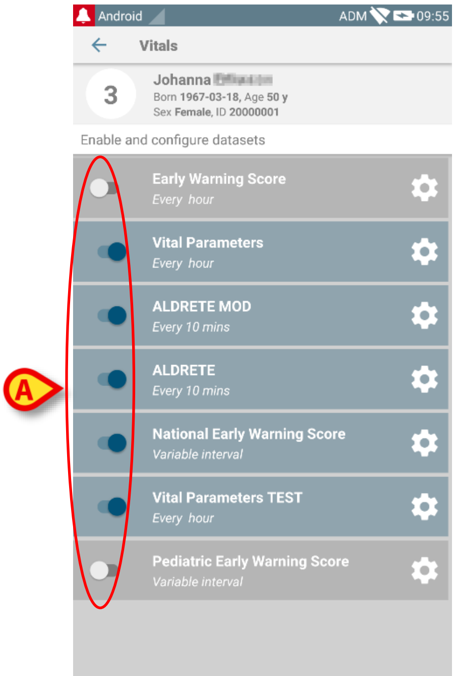
Vital Parameters
Every 60 minutes, due at 25-08-2017 16:09

ALDRETE MOD
Every 10 minutes, due NOW

Vital Parameters TEST
Every 60 minutes, due at 28-08-2017 15:00

Fig 95

The list of all the existing datasets (defined by configuration) will open (Fig 96). The list of all existing dataset is configured.


Android ADM 09:55

Vitals

3 Johanna [redacted]
Born 1967-03-18, Age 50 y
Sex Female, ID 20000001

Enable and configure datasets

Early Warning Score
Every hour

Vital Parameters
Every hour

ALDRETE MOD
Every 10 mins

ALDRETE
Every 10 mins

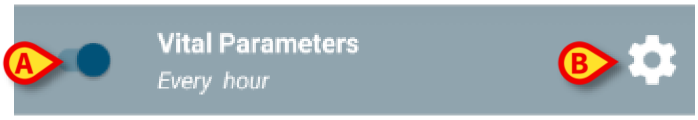
National Early Warning Score
Variable interval

Vital Parameters TEST
Every hour

Pediatric Early Warning Score
Variable interval

Fig 96

Use the switch on the left to enable/disable a dataset for the selected patient (Fig 96 **A**).
The switch is dark blue and positioned on the right when the dataset is enabled (Fig 97 **A**).



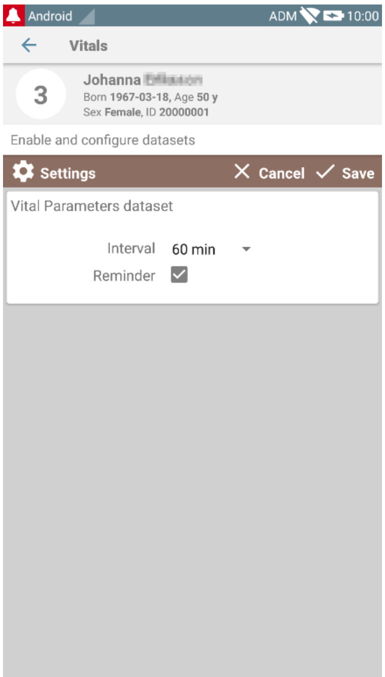
Vital Parameters
Every hour

Fig 97

For each dataset the name and the current configuration settings are displayed.

- ➢ Touch the ⚙ icon to configure the dataset (Fig 97 **B**).

The following screen will open (Fig 98).



3 Johanna [redacted]
Born 1967-03-18, Age 50 y
Sex Female, ID 20000001

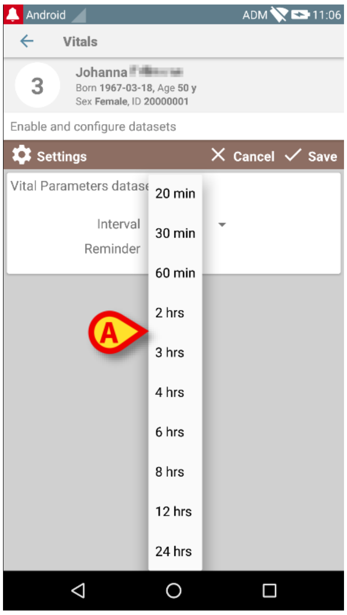
Enable and configure datasets

Vital Parameters dataset

Interval 60 min
Reminder ☑

Fig 98

- ➢ Touch the "Interval" menu to decide the dataset timing (Fig 99).



3 Johanna [redacted]
Born 1967-03-18, Age 50 y
Sex Female, ID 20000001

Enable and configure datasets

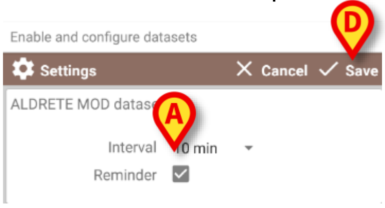
Vital Parameters datase

Interval

Reminder

Fig 99

- ➢ Select the “Reminder” checkbox to get automatic reminders on when the datasets acquisitions are due (Fig 100 **A**).



Enable and configure datasets

ALDRETE MOD datase

Interval 10 min

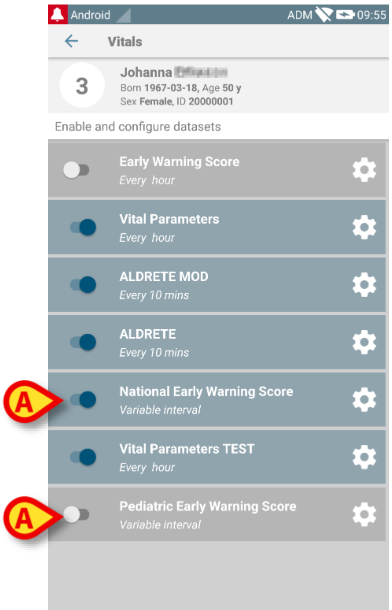
Reminder ☑

Fig 100

After configuring the dataset,

- ➢ Touch the **Save** option to save the changes made (Fig 100 **B**).
- ➢ Touch **Cancel** to go back to the datasets list.

Some datasets are pre-configured on a single timing option (i.e. “Once” or “Variable Interval” - see Fig 101 **A**).



3 Johanna [redacted]
Born 1967-03-18, Age 50 y
Sex Female, ID 20000001

Enable and configure datasets

Early Warning Score
Every hour

Vital Parameters
Every hour

ALDRETE MOD
Every 10 mins

ALDRETE
Every 10 mins

National Early Warning Score
Variable interval

Vital Parameters TEST
Every hour

Pediatric Early Warning Score
Variable interval

Fig 101

8. DIGISTAT® “Voice Notes”

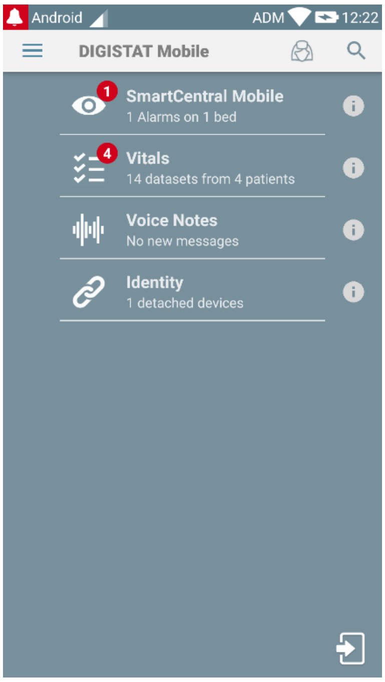
8.1 Introduction

The “Voice Notes” module makes it possible to record vocal notes associated to the patients, with selectable topics and a configurable message lifespan.

8.2 Application start-up

To start the “Voice Notes” module:

- ➢ Touch the corresponding row on the handheld device screen (Fig 102).



Android ADM 12:22

DIGISTAT Mobile

SmartCentral Mobile
1 Alarms on 1 bed

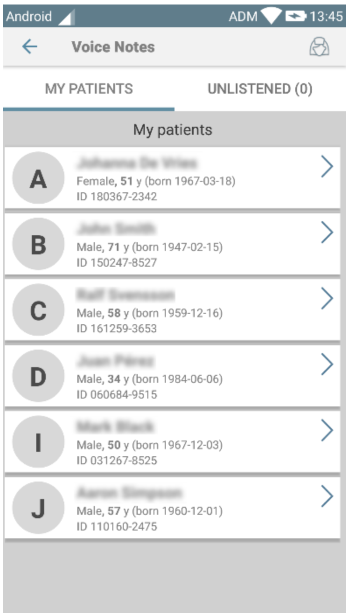
Vitals
14 datasets from 4 patients

Voice Notes
No new messages

Identity
1 detached devices

Fig 102

The “Voice Notes” screen is shown in Fig 103.


Android ADM 13:45

Voice Notes

MY PATIENTS UNLISTENED (0)

My patients

A [redacted]
Female, 51 y (born 1967-03-18)
ID 180367-2342

B [redacted]
Male, 71 y (born 1947-02-15)
ID 150247-8527

C [redacted]
Male, 58 y (born 1959-12-16)
ID 161259-3653

D [redacted]
Male, 34 y (born 1984-06-06)
ID 060684-9515

I [redacted]
Male, 50 y (born 1967-12-03)
ID 031267-8525

J [redacted]
Male, 57 y (born 1960-12-01)
ID 110160-2475

Fig 103

This screen lists al the patients existing in the handheld device domain.

8.2.1 Users access

The “Voice Notes” requires a valid user logged in to be used. If no user is logged, the related row in the Digistat Mobile main screen is like the one reported in Fig 104.

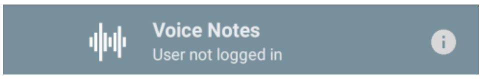
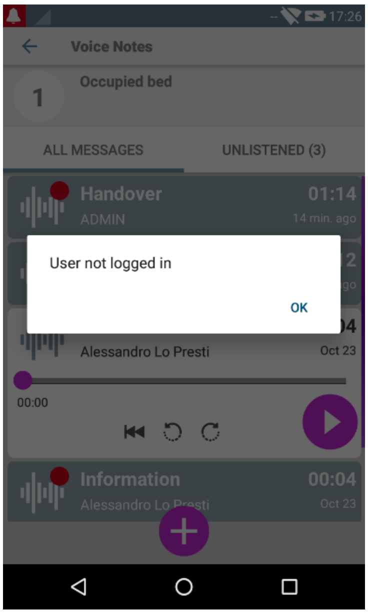

Voice Notes
User not logged in

Fig 104

It’s not possible to use “Voice Notes" if the same user is currently logged in another device. If this happens, the user is automatically logged out from the device previously logged in: in such case a pop-up notification is shown notifying the disconnection, as indicated in Fig 105.



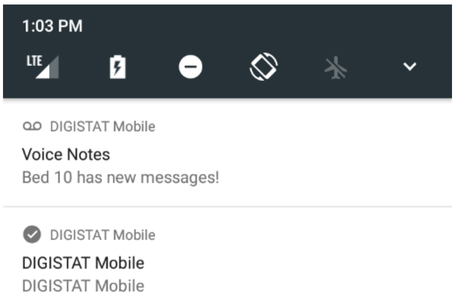
User not logged in

OK

Fig 105

8.2.2 Notifications

At the application start up or when there's a new message, the system shows a notification. Clicking on the notification opens the patient screen with the messages list (Fig 106).



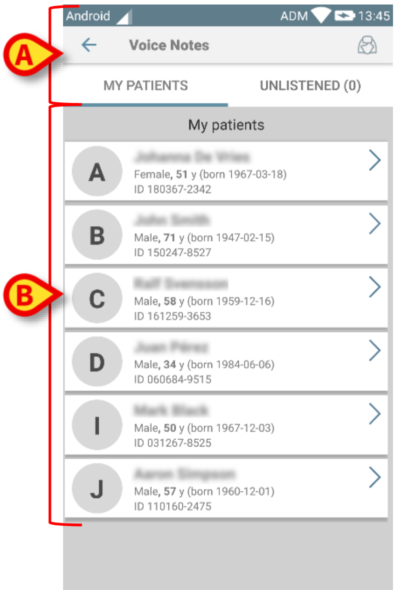
DIGISTAT Mobile
Voice Notes
Bed 10 has new messages!

DIGISTAT Mobile
DIGISTAT Mobile
DIGISTAT Mobile

Fig 106

8.3 Patients list

The “Voice Notes” patient list screen (Fig 107) shows the list of beds configured on the handheld device (namely, the device “domain”). The domain of a specific handheld device is defined by configuration.



Android ADM 13:45

Voice Notes

MY PATIENTS UNLISTENED (0)

My patients

A [redacted]
Female, 51 y (born 1967-03-18)
ID 180367-2342

B [redacted]
Male, 71 y (born 1947-02-15)
ID 150247-8527

C [redacted]
Male, 58 y (born 1959-12-16)
ID 161259-3653

D [redacted]
Male, 34 y (born 1984-06-06)
ID 060684-9515

I [redacted]
Male, 50 y (born 1967-12-03)
ID 031267-8525

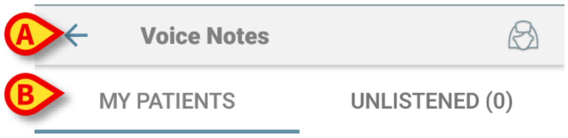
J [redacted]
Male, 57 y (born 1960-12-01)
ID 110160-2475

Fig 107

In case there is no patient on one of the configured beds, then the bed is not displayed. The patient list screen is formed of a heading (Fig 107 **A**) and the patients list (Fig 107 **B**).

8.3.1 Patient list heading

Fig 108 shows the heading of the patient list screen.



Voice Notes

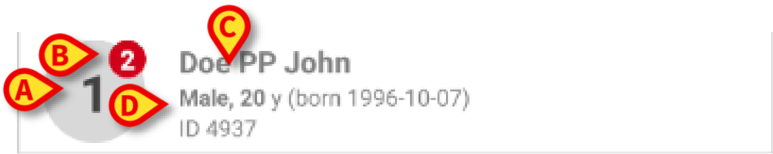
MY PATIENTS UNLISTENED (0)

Fig 108

Touch the left arrow indicated in Fig 108 **A** to exit the module and display the handheld device screen (Fig 102). Use the filter indicated in Fig 108 **B** to display either all the patients configured on the handheld device domain or only the patients for which there are unlistened voice messages (**Unlistened**) for the current logged user.

8.3.2 List of beds

Each bed is represented by a tile (Fig 109).



Doe PP John
Male, 20 y (born 1996-10-07)
ID 4937

Fig 109

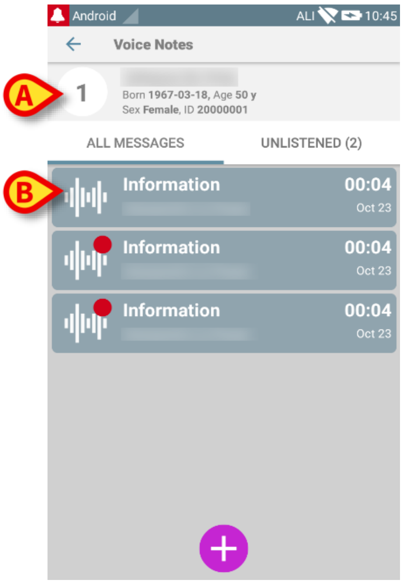
In the tile, the following information are available:

- bed number (Fig 109 **A**);
- number of unlistened messages (if any) (Fig 109 **B**);
- name of patient on that bed (Fig 109 **C**);
- patient data (if available: sex, age, date of birth, patient ID - Fig 109 **D**).

Touch one tile to access the list of voice messages for the corresponding patient.

8.4 Voice messages list

The voice messages list screen is formed of two areas: a heading area (Fig 110 **A**) and the list of voice messages (Fig 110 **B**).



Born 1967-03-18, Age 50 y
Sex Female, ID 20000001

Information 00:04 Oct 23
Information 00:04 Oct 23
Information 00:04 Oct 23

Fig 110

The heading area displays the following information:

- bed number;
- name of patient on that bed;
- patient data (if available: sex, age, date of birth, patient ID).

The voice messages are displayed in tiles below the heading area. Each tile represents a voice message. Fig 111 shows some examples.

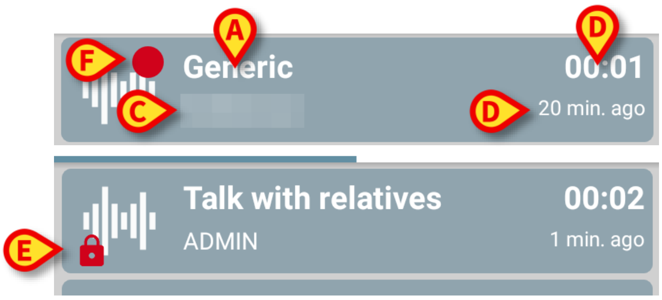


Fig 111

The voice message tile displays the following information (Fig 111):

- **A**: subject of the message;
- **B**: duration of the message;
- **C**: the author: i.e. the user who has recorded the message;
- **D**: creation time: when the voice message has been recorded.
- **E**: the padlock icon (optionally shown) indicates that the message has been marked as private. It means that only the author can see this entry and listen to it
- **F**: the red circle icon (optionally shown) indicates that the message has not been listened yet).

8.4.1 Listening to voice messages

To listen to a voice message

- ➢ touch the message tile;

The tile expands to show the audio player control buttons (Fig 112 and Fig 113).

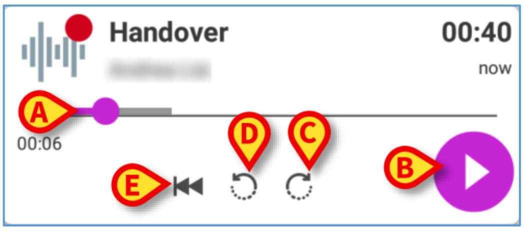


Fig 112 – unlistened voice message

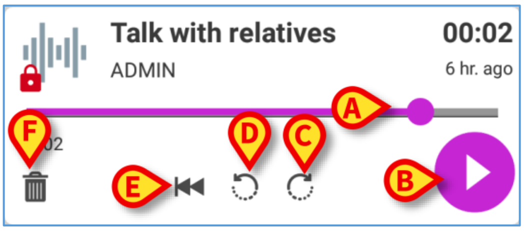


Fig 113 - private message, deletable by the author

In the following are detailed the control buttons:

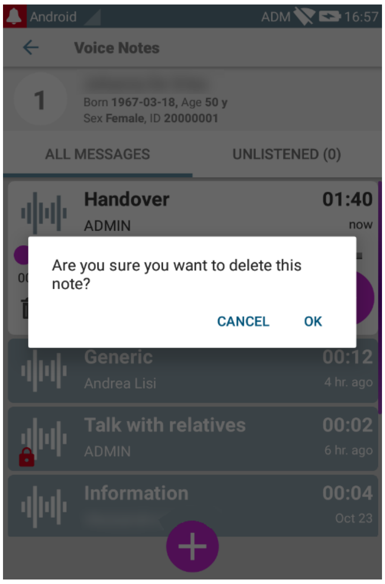
- seekbar (Fig 112 and Fig 113 **A**): touch the thumb and drag left or right to set the current progress level;
- play the message (Fig 112 and Fig 113 **B**);
- skip 10 seconds forward (Fig 112 and Fig 113 **C**);
- skip 10 seconds backward (Fig 112 and Fig 113 **D**);
- go back to the beginning (Fig 112 and Fig 113 **E**);
- delete the message (optionally shown - Fig 113 **F).**

Note:

- ❖ A confirmation icon ✓ (in the same place of the symbol Fig 113 **F**) if present, makes it possible to mark the note as “listened”. Touch the icon to mark the note as “listened”;
- ❖ It is allowed to skip forward in the message only till the last listened position. The part of the message listened is highlighted on the seekbar with a thicker gray line;
- ❖ When clicking on a message tile, on the expanded view, the system automatically sets the begin point of the audio player seek bar at the last listened position.

8.4.2 Delete a voice message

Voice messages are automatically deleted after their life time. Deleted messages are not recoverable. Only the author is allowed to delete his/her messages before the expiration time, by clicking on the icon 🗑, situated in the expanded message view (see Fig 113). This operation requires a confirmation (Fig 114):



Born 1967-03-18, Age 50 y
Sex Female, ID 20000001

Handover 01:40
ADMIN now

Are you sure you want to delete this note?

Generic 00:12
Andrea Lisi 4 hr. ago

Talk with relatives 00:02
ADMIN 6 hr. ago

Information 00:04
Oct 23

Fig 114

If some user in the network is listening to a message while it’s being deleted, a message alert is shown.

8.4.3 Record a voice message

To record a voice note, select the patient on the Patient List screen (Fig 107). The following screen will be displayed (Fig 115), listing all the notes currently existing for the selected patient (in Fig 115 no note exists).

Touch the ⊕ icon placed at the bottom of the page, as indicated in Fig 115:

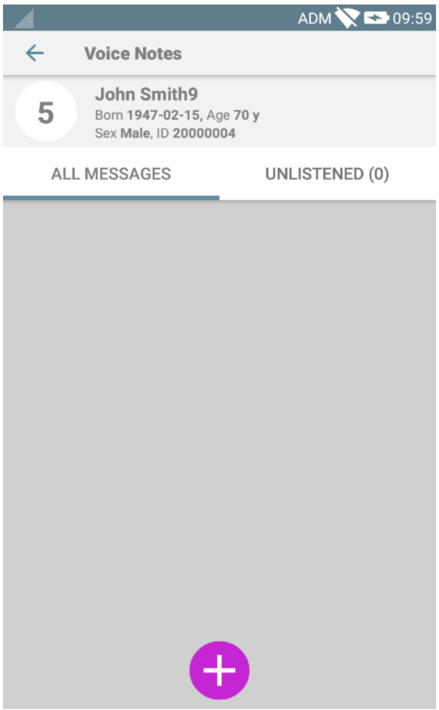
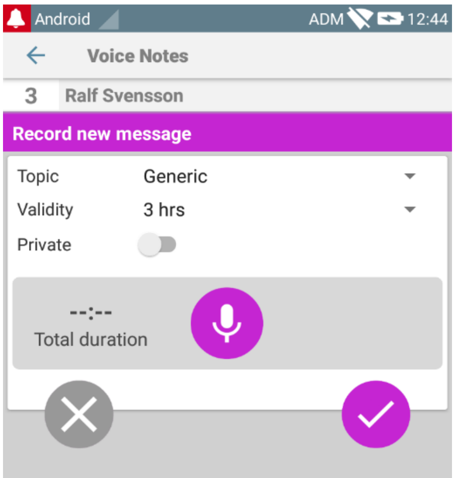


Fig 115

The recording screen will open as shown in Fig 116:



Topic Generic
Validity 3 hrs
Private

Fig 116

Before recording a note, it is possible to select the note topic on a pre-defined list (Fig 117):

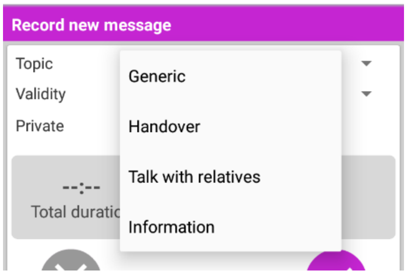


Fig 117

Also, before recording a note, it is possible to define the note's lifespan. Messages are automatically deleted after the time span specified here (Fig 118).

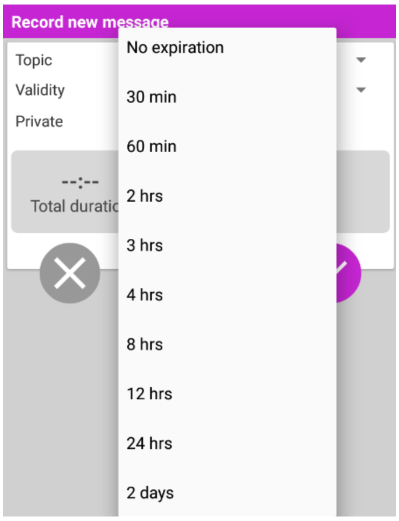
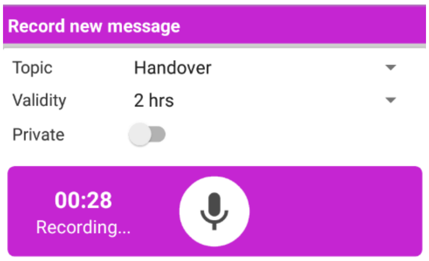


Fig 118

To record a new voice message:

- ➢ keep pressed the button 🎤 as indicated in Fig 119:



Topic Handover

Validity 2 hrs

Private

Fig 119

The button turns to white while recording. The recording time is displayed alongside the button. Recording stops when the button is released (Fig 120). The default maximum registration length is 5 minutes (configurable value). If necessary, it is possible continue recording by again pressing the record button.

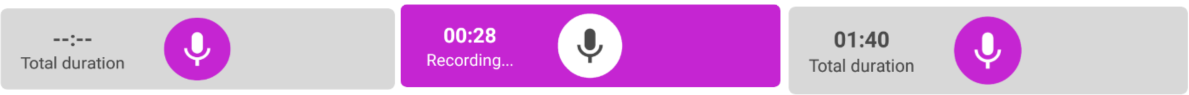
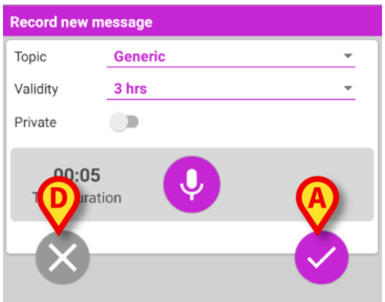


Fig 120

When the recording is completed, it's possible to save the message by clicking the button ✓ (Fig 121 **A**) or cancel the operation and discard the message by clicking the button ⊗ (Fig 121 **B**).



Record new message

Topic: Generic

Validity: 3 hrs

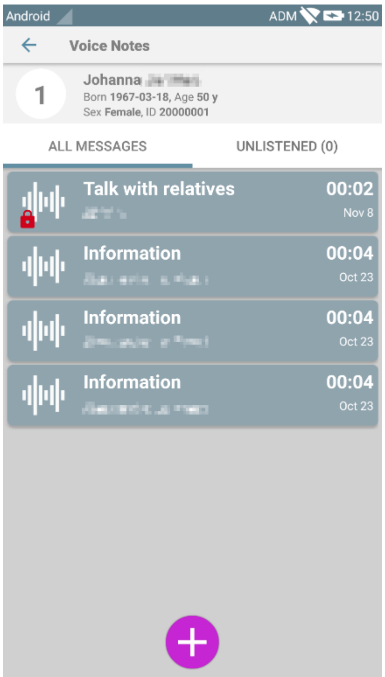
Private

00:05

Total duration

Fig 121

After saving, the messages list screen of the selected patient is displayed again, including the last recorded note (Fig 122).



Android ADM 12:50

Voice Notes

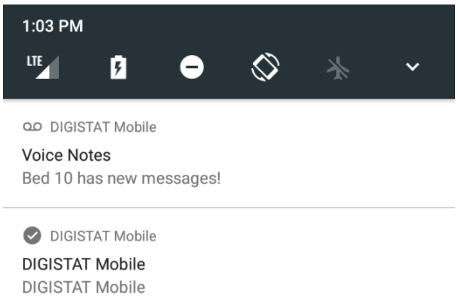
1 Johanna [redacted]
Born 1967-03-18, Age 50 y
Sex Female, ID 20000001

ALL MESSAGES UNLISTENED (0)

Talk with relatives [redacted]	00:02	Nov 8
Information [redacted]	00:04	Oct 23
Information [redacted]	00:04	Oct 23
Information [redacted]	00:04	Oct 23

Fig 122

When a new message is saved, a notification is displayed on the other handheld devices having the same bed in their domain (Fig 123).



1:03 PM

DIGISTAT Mobile
Voice Notes
Bed 10 has new messages!

DIGISTAT Mobile
DIGISTAT Mobile
DIGISTAT Mobile

Fig 123

The same notification is displayed at application start-up as well. Touch the notification to display the messages list screen (Fig 123).

9. DIGISTAT® "Identity"

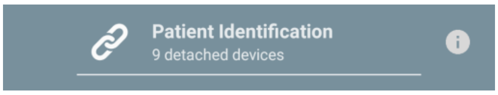
9.1 Introduction

The "Identity" module allows users to establish or delete the assignment of one or more devices to a patient. The "Identity" module satisfies the need to dispose of devices usually not associated with a bed and that can be moved around changing their association. Setting or deleting the assignment of devices to a patient is performed by means of patients and devices identification using the barcode scanning through the mobile device camera or using the device NFC capabilities, if available.

Note: "Identity" doesn't work when patient anonymization is enabled, i.e. it cannot be used on patients whose personal data are not available for the current user: in these conditions a safe patient identification could not be performed. For the same reason, "Identity" cannot be used if no user is logged in. External events triggering user disconnection would also kick the user out of the module.

9.2 Application Start-Up

In Fig 124 is shown the "Identity" launcher row in the DIGISTAT® "Mobile" main screen:

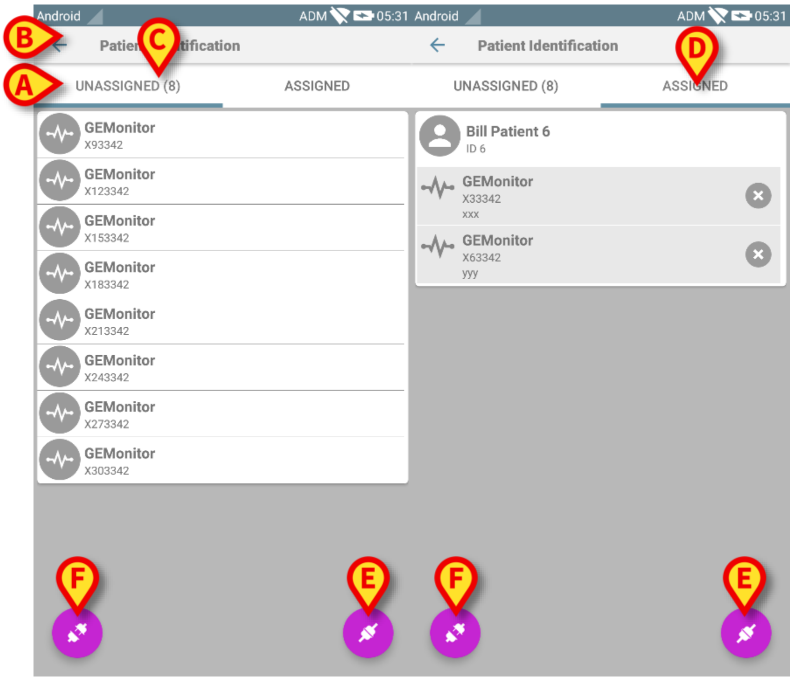


Patient Identification
9 detached devices

Fig 124

9.2.1 Main view

“Identity” main view is divided in two tabs that can be selected using the filter in Fig 125 **A**:



GEMonitor X93342

GEMonitor X123342

GEMonitor X153342

GEMonitor X183342

GEMonitor X213342

GEMonitor X243342

GEMonitor X273342

GEMonitor X303342

Bill Patient 6 ID 6

GEMonitor X33342 xxx

GEMonitor X63342 yyy

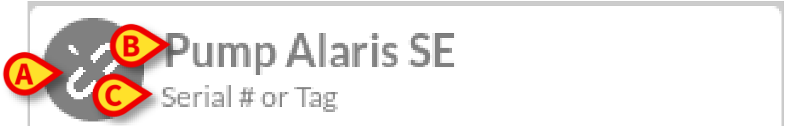
Fig 125

The first tab shows the list of unassigned devices (Fig 125 **C**), while the second one shows the current status of the assigned devices (Fig 125 **D**).

At the bottom of the main view there are two icons, a 🔌 and an 🔌. Tapping on the first one (Fig 125 **E**) the process to establish the association between patient and device will be started; tapping on the second one (Fig 125 **F**) the process to delete the association between patient and device will be started.

9.2.2 List of unassigned device

In Fig 125 **C**, each item in the list is related to an unassigned device. In Fig 126 an unassigned device is considered.



Pump Alaris SE

Serial # or Tag

Fig 126

An icon represents the device type: if it is known, these symbols are the same ones used in the Smart Central module for the device connected to patient (see Paragraph 0); otherwise, a broken link icon is shown (Fig 126 **A**). It is also shown the device name (Fig 126 **B**), the serial number and the label (if available - Fig 126 **C**). The label is the device code used to identify the device.

9.2.3 List of assigned device

In Fig 125 **D**, each item in the list is related to a patient. In Fig 127 is considered a patient at which is associated an assigned device.

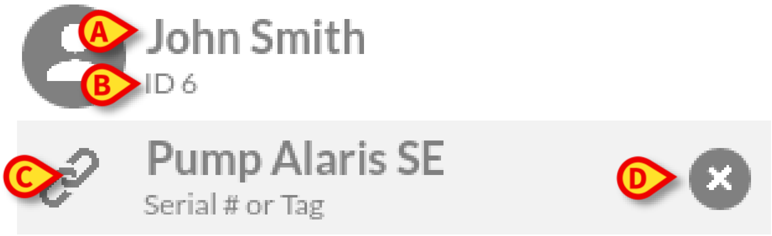


Fig 127

In Fig 127 the patient name (Fig 127 **A**) and the patient identification code (Fig 127 **B**) are detailed for the user. By clicking on the patient row it is possible to expand the list of all devices associated to the patient (Fig 127 **C**). Each associated device has an icon representing its type, name, serial number and the label (see Paragraph 9.2.2 for the details). Finally there is an ⊗ icon on the right side of the device entry (Fig 127 **D**) to allow the user a quick disassociation of the device from the patient.

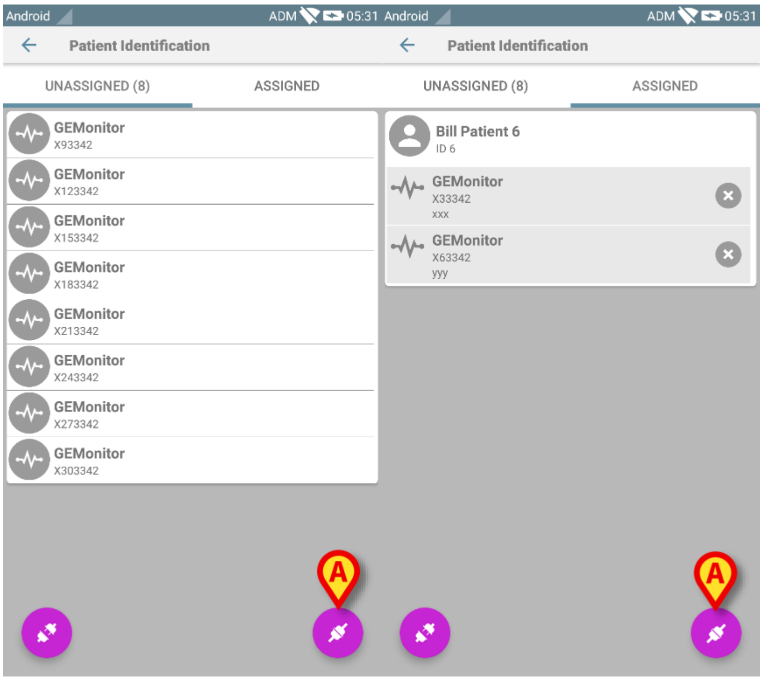
9.3 Set association workflow

The process establishing the association between patient and devices is detailed as follows:

1. Start of the process from the main screen;
2. Patient identification (via barcode or NFC tag);
3. Confirmation of patient identified;
4. Device identification (via barcode or NFC tag);
5. Confirmation of device identified.

9.3.1 Start of the process

In the main screen of the “Identity” module, the user has to click on the 🔌 icon (Fig 128 **A**):



GEMonitor X93342
GEMonitor X123342
GEMonitor X153342
GEMonitor X183342
GEMonitor X213342
GEMonitor X243342
GEMonitor X273342
GEMonitor X303342

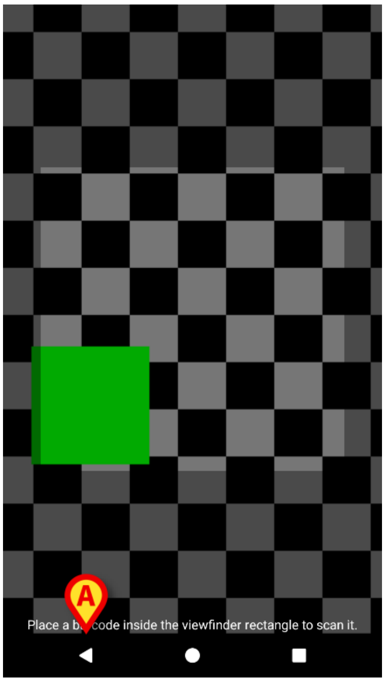
Bill Patient 6 ID 6
GEMonitor X33342 xxx
GEMonitor X63342 yyy

Fig 128

The association process is now started: the user has to identify the patient for which the association is requested.

9.3.2 Identification of the patient

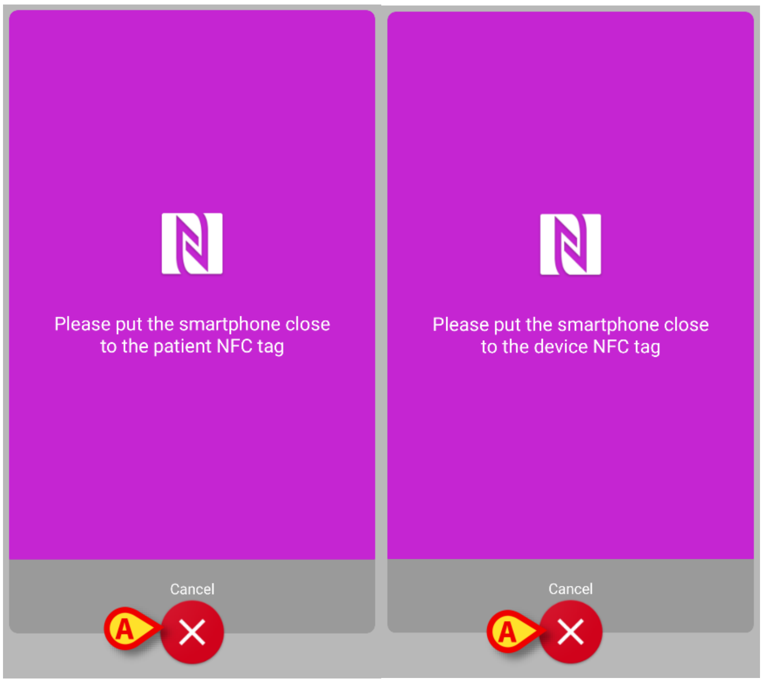
According to the Healthcare Organization configuration, it is equally possible to identify patients scanning its barcode or its NFC tag. A message is displayed reminding which kind of barcode / NFC tag is going to be scanned (if patient or device).
In Fig 129 is shown the screen view of the barcode scanning. Touching the button in Fig 129 **A** it is possible to stop the identification procedure.



Place a barcode inside the viewfinder rectangle to scan it.

Fig 129

In Fig 130 is show the screen view of the NFC tag scanning (for patient and device, respectively). Touching the button in Fig 130 **A** it is possible to stop the identification procedure.



Please put the smartphone close to the patient NFC tag

Please put the smartphone close to the device NFC tag

Fig 130

If the patient identification is not possible, a notification is shown to inform the user.

9.3.3 Confirmation of patient identification

A screen view is provided for the user showing the patient main data and a photo of the patient (if available; otherwise, a generic icon is displayed - Fig 133):

- Patient name, birth date, age, sex, identification code (Fig 133 **A**);
- Patient photo (Fig 133 **B**).

Since a patient photo is missing, by touching the button in Fig 133 **C** it is possible to take a new one. Once a new photo is taken, it is possible to modify it with the aim to select a reduced area suitable to the detailed patient screen view. In Fig 131 is showed the screen of a high resolution screen device (i.e. not a Myco 1/2).

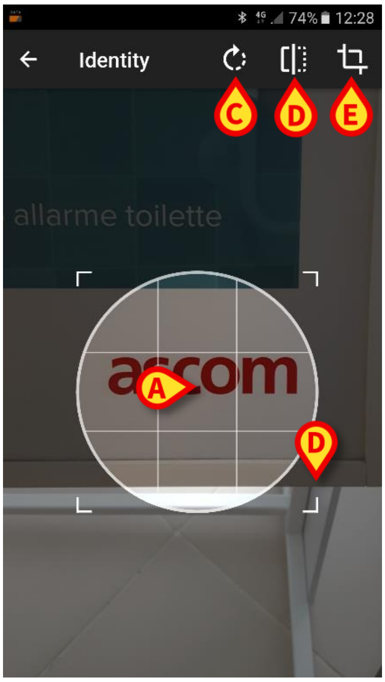


Fig 131

The whole procedure was designed in order to allow the user to make any change by means of one finger. The user can move the lattice area by touching and dragging the center of the lattice (Fig 131 **A**). Moreover, the user can change the lattice area size by touching and dragging the bottom right corner (Fig 131 **B**). Furthermore, the user can rotate the picture ((Fig 131 **C**) or flip it (Fig 131 **D** – a menu allows to choose if horizontally or vertically). After the changes, the user can confirm them by touching the icon in Fig 131 **E**.

In Fig 132 are shown screenshot taken during same operations now explained performed on Myco 1/2 devices (i.e. low resolution screens). The only difference is that the user can perform rotation/flip operations by means of the button in the red circle in Fig 132 **G**.

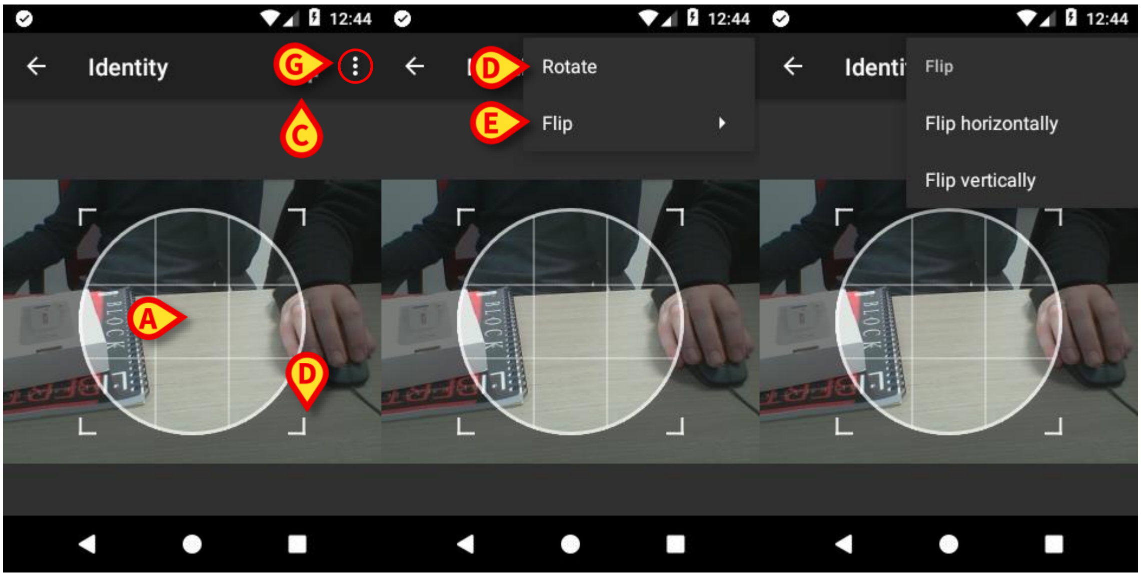
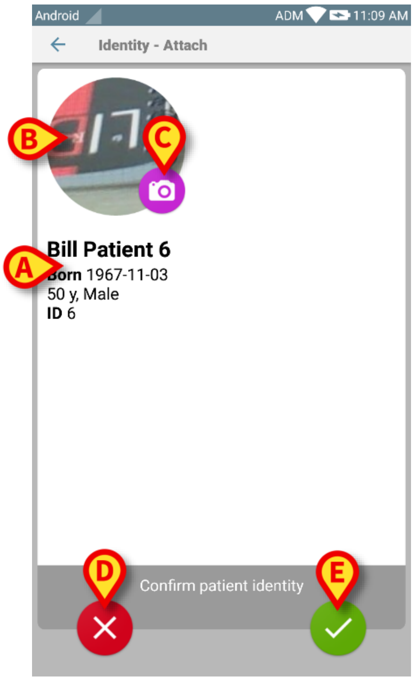


Fig 132

Finally it is possible to delete the patient photo by long touching it.
The user can deny or confirm the suggested patient identification by touching respectively the buttons in Fig 133 **D** or Fig 133 **E**. If the patient identification is denied, then the procedure is deleted. If the user has updated the patient photo and the patient identification is denied, then the patient photo update is also denied.



Bill Patient 6
Born 1967-11-03
50 y, Male
ID 6

Fig 133

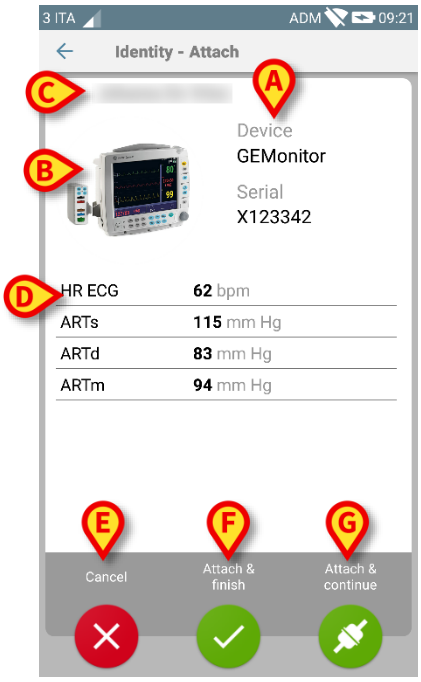
After the confirmation of the patient identification, the user is requested to identify one or more device with which establish (or delete) the association.

9.3.4 Device identification

The device identification is performed according to the same procedure of the patient identification (see paragraph 9.3.2). If the device identification is not possible (i.e.: device not found; device associated to another patient), the procedure is stopped.

9.3.5 Confirmation of device identification

A screen view is provided for the user, showing the device main data (Fig 134 **A**) and an image of the device (if available; otherwise, a generic icon is displayed - Fig 134 **B**). In Fig 134 **C** it is shown the name of the patient with which the association has to be set (or unset; see paragraph 9.4). If it foreseen from the Healthcare Organization configuration, in Fig 134 **D** it is possible to show the real time data provided by the device; if no data are coming from the device, instead of device data an error string is shown.
In the Fig 134 are present three buttons. With the button in Fig 134 **E** it is possible to deny the device identification and go back to the device search. With the button in Fig 134 **F** it is possible to confirm the device identification and then conclude the association procedure. With the button in Fig 134 **G** it is possible to confirm the device identification and go back to identify a new device.



Device
GEMonitor

Serial
X123342

HR ECG	**62** bpm
ARTs	**115** mm Hg
ARTd	**83** mm Hg
ARTm	**94** mm Hg

Fig 134

9.4 Unset association workflow

The process deleting the association between patient and devices is detailed as follows:

1. Start of the process from the main screen;
2. Device identification (via barcode or NFC tag);
3. Confirmation of device identified;
4. Further identification of other devices (repeat steps 2 and 3);
5. End of process.

9.4.1 Start of the process

In the main screen of the “Identity” module, the user has to click on the icon (Fig 135 **A**):

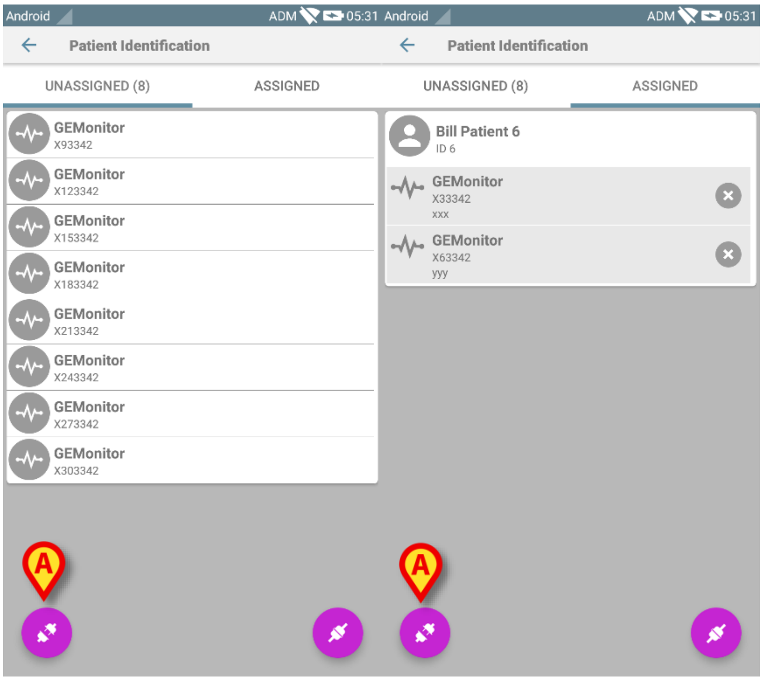


Fig 135

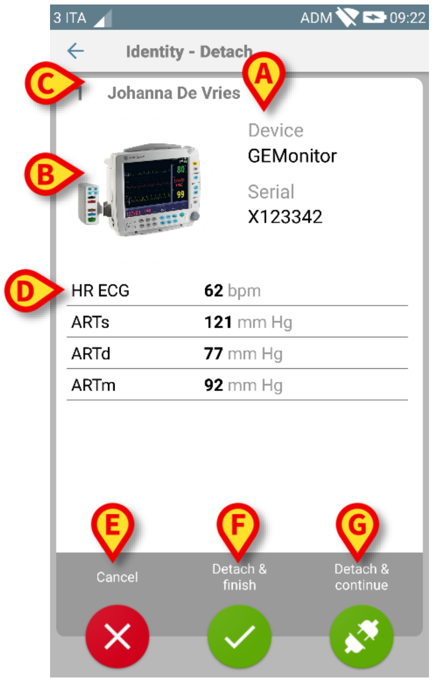
The cancellation of the association is now started: the user has to identify the device for which the association cancellation is requested.

9.4.2 Device identification

The device identification is described in paragraph 9.3.4.

9.4.3 Confirmation of device identification

The procedure to confirm the device identification is the same described in paragraph 9.3.5. Nonetheless, the displayed screen is slightly different because of the button labels (Fig 136):



Johanna De Vries

Device
GEMonitor

Serial
X123342

HR ECG	62 bpm
ARTs	121 mm Hg
ARTd	77 mm Hg
ARTm	92 mm Hg

Fig 136

10. Manufacturer Contacts

For any issue, please refer first to the Distributor who installed the Product.
Here are the manufacturer contacts:

ASCOM UMS s.r.l unipersonale
Via Amilcare Ponchielli 29, 50018, Scandicci (FI), Italy
Tel. (+39) 055 0512161
Fax (+39) 055 8290392

Technical assistance
support.it@ascom.com
800999715 (toll free, Italy only)

Sales and products information
it.sales@ascom.com

General info
it.info@ascom.com

11. Residual risks

A risk management process has been implemented in the life cycle of DIGISTAT® [SI1] adopting the relevant technical regulations (EN14971, EN62304, EN62366). The risk control measures have been identified and implemented in order to reduce the residual risks to the minimum level and make them acceptable compared to the benefits brought in by the product. The total residual risk is also acceptable if compared to the same benefits.

The residual risks listed below have been taken into consideration and reduced to the minimum level possible. Given the inherent nature of the "risk" concept, it is not possible to completely remove them. It is therefore necessary, according to the regulations, to let the users know each and every possible risk (even though remote).

- Inability to using the system or some of its functionalities, which can cause delays and/or errors in the therapeutic/diagnostic actions.
- Slowdown of DIGISTAT® performance, which could cause delays and/or errors in the therapeutic/diagnostic actions.
- Circulation of users' and/or patients' sensitive data.
- Unauthorized actions carried out by users, which can cause errors in the therapeutic/diagnostic actions and in the allocation of responsibilities of these actions.
- Wrong data insertion and display, which can cause errors in the therapeutic/diagnostic actions.
- Display of either partial or hard-to-read information, which can cause delays and/or errors in the therapeutic/diagnostic actions.
- Attribution of device data to the wrong patient (patient exchange), which can cause errors in the therapeutic/diagnostic actions.
- Accidental data deletion, resulting in loss of data, which can cause delays and/or errors in the therapeutic/diagnostic actions.

RISKS RELATING TO THE HARDWARE PLATFORM IN USE

- Electric shock for the patient and/or the user, which can cause injury and/or death for the patient/user.
- Hardware components overheating, that can cause injury for the patient/user.
- Infection contraction for the patient/user.