DIGISTAT® Mobile
User Manual

DIGISTAT® V4.3

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 4.3

SOFTWARE LICENSE

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

WARNING

The information contained herein is subject to change without further notice. ASCOM UMS holds the right to make changes to all described products in order to improve its functions and performance.

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 to UNI EN ISO 9001:2008 and UNI CEI EN ISO 13485:2012 standards for the design, development, production, installation and servicing of software.

Contents

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 5”) or to a paragraph / section (e.g. “paragraph 2.2.1”), 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 7 **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 elements of a list.

1.3 Symbols

The following symbols are used in this manual.

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.

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 Modular Architecture

"Modular Architecture" means that different products (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.

2.2 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.

2.2.1 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.

2.3 "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".

2.4 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 health 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.

2.5 Manufacturer's responsibility

The CE Marking is a declaration that the Product complies with the applicable Directives and Regulations.
ASCOM UMS is responsible for the product's safety, reliability and performance only if:

- Use and maintenance comply with User Manual instructions;
- This Manual is stored in good conditions and all sections are readable;
- Configurations, changes and repairs are only performed by personnel formed and authorized by ASCOM UMS ;
- The Product's usage environment complies with safety regulations;
- The electrical wiring of the environment where the Product is used complies with applicable regulations and is efficient.

! Should the electrical supply cause the establishment of a "medical electrical system" through electrical and functional connection of devices, the healthcare facility is in charge of the required safety verification and acceptance tests, even where ASCOM UMS performed in whole or in part the wiring and the necessary connections.

2.6 Product tracking

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).

2.7 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.

2.8 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

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.

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 (1280 x 1024 suggested, 65.000 colors minimum)
- 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
- Monitor: 1024 x 768 or higher (1280 x 1024 suggested, 65.000 colors minimum)
- Mouse or other compatible device
- Ethernet interface 100 Mb/s (or higher)
- 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

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 (build from 5.3.0 to 6.5.1). The application may be compatible with other Android devices, but such compatibility should be tested and validated before the release.

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

3.4 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.

In compliance with ongoing product improvement policies pursued by ASCOM UMS, this User Manual's specifications can be changed at any moment.

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.

3.4.1 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 software is installed and regularly updated both on the client PCs and the server.

The Responsible Organization shall ensure that these two protections are activated. ASCOM UMS tested the Product with ESET Antivirus but, considering the strategies and policies already existing in the healthcare facility, 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.

3.5 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 backbones 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 facility 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.

3.5.1 DIGISTAT® system impact on the healthcare facility network

DIGISTAT® system impacts the local network of the healthcare facility. 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.

In a configuration with 100 client PCs the following bandwidth occupation values can be indicatively predicted.

Average: 0.8 – 6 Mbit/s

Pitch: 5 – 25 Mbit/s

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.

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).

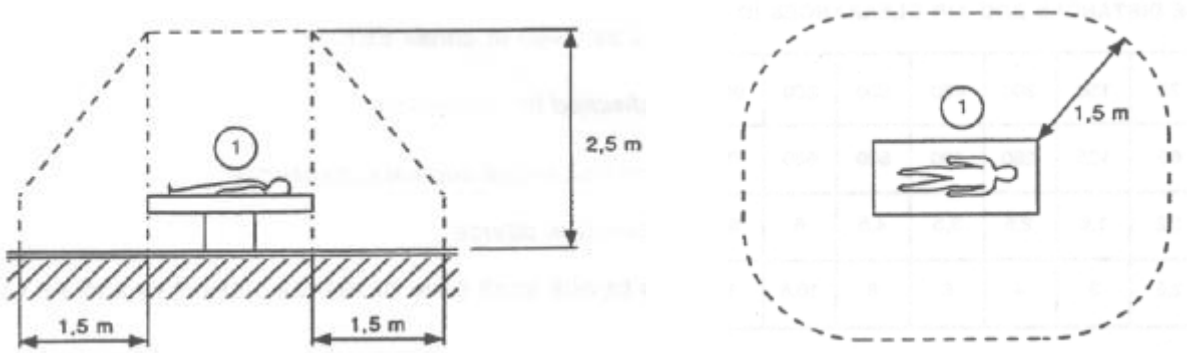

Fig 1 - Patient Area

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 installation result in the establishment of a "medical electrical system" through electrical and functional connection of devices, the responsible organization is in charge of the required safety verification and acceptance tests. This responsibility applies even where ASCOM UMS/Distributor performed in whole or in part the wiring and the necessary connections.

4.2 Cleaning

Cleaning and disinfection procedures of hardware components must comply with the usual cleaning/disinfection procedures that the healthcare facility adopts for all the healthcare facility'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 responsible 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.

The electrical devices installed within the Patient Area (see Fig 1) must have the same security level of an electro-medical 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 facility is responsible for these measurements.

The healthcare facility 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

The following precautions should 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.

"Sensitive data" is personal data that reveal the race, the religious and/or philosophic beliefs, the personal political opinions, the support to political parties and/or trade unions and/or associations and organizations having political, religious or philosophical aims. Moreover, "sensitive data" is data providing information on the health conditions and/or the sexual life of individuals.

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.
- Sensitive data saved in the system, such as 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 facility is responsible for implementing this software and keep them updated.

In some circumstances, personal and/or sensitive 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 facility is responsible for providing adequate security measures to comply with the local privacy laws and regulations.

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 (D.Lgs 196/2003 of the 30th of June 2003).

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 responsible 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 responsible 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 responsible 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

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 facility 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 facility 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 facility 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 facility 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 facility’s authorized staff replaces the out of order PC with the “substitution equipment”
2) The healthcare facility 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 facility 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 facility. 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

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 facility 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 facility 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 facility 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 8 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 paragraph 5.7 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 2 is referring to a scenario where the ASCOM Myco is integrated with UNITE.

5.2.1 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.

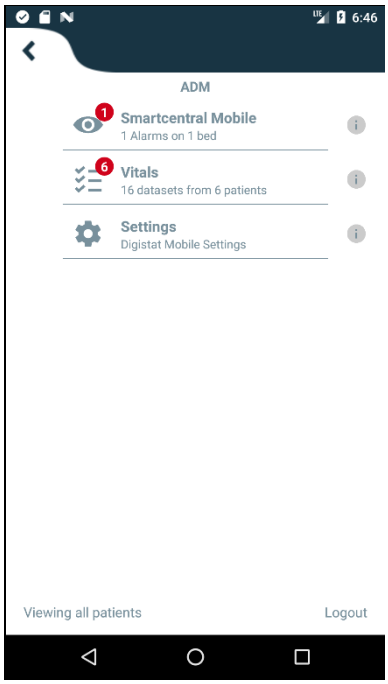

Fig 2

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 3).

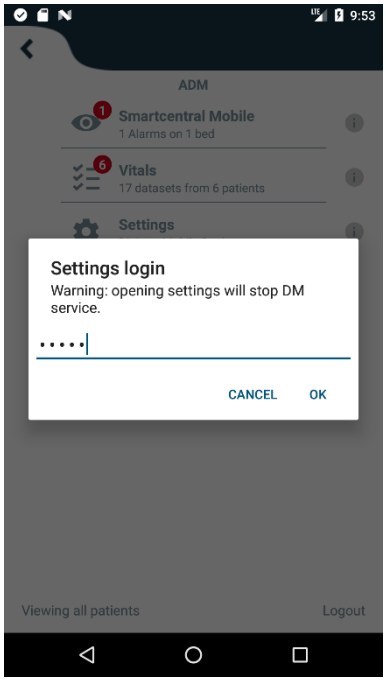

Fig 3

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

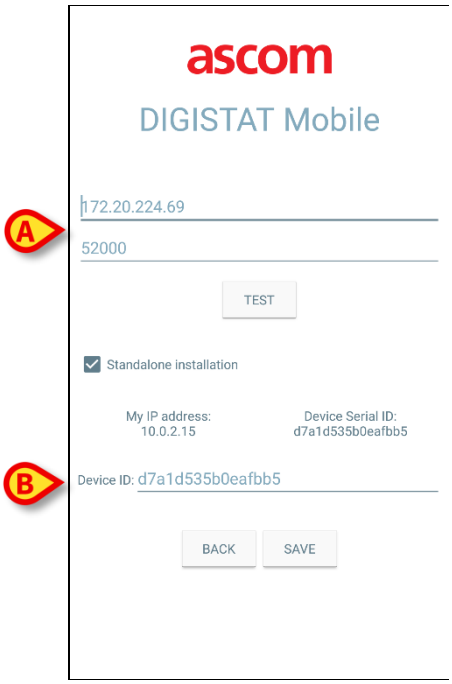

Fig 4

It is here possible to specify the IP address of the server and the server port (Fig 4 **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 4 **B**) makes it possible to change the device id code.

5.2.2 Android device start-up

On the handheld device,

- Touch the  icon.

The following screen will be displayed (Fig 5).

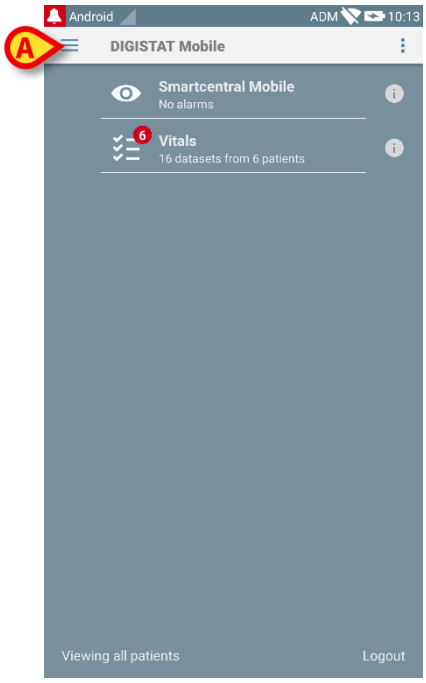

Fig 5

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 6 - see paragraph 5.3 for the full list of options).

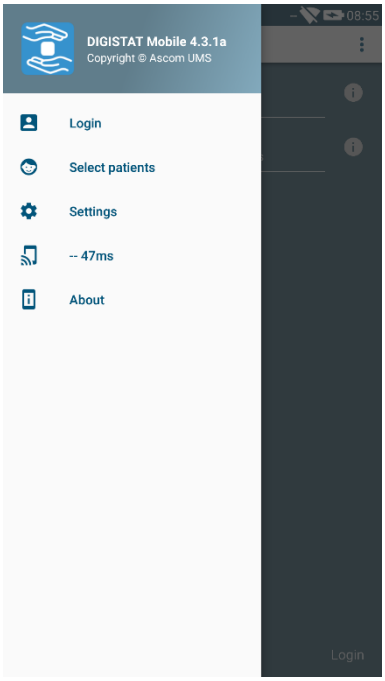

Fig 6

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

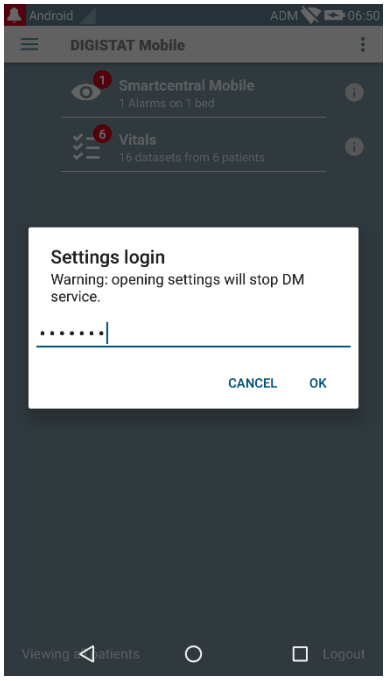

Fig 7

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

Fig 8

It is here possible to specify the IP address of the server and the server port (Fig 4 **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 8 **B**) makes it possible to change the device id code.

5.2.3 Updates installation (APK files)

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

Fig 9

To install the software updates

- Touch the row indicated in Fig 9 **A**.

5.3 Lateral Menu

NOTE: the lateral menu is only available on non-Myco devices or Mycos not connected with UNITE.

The  icon on the top-left corner opens a menu containing different options (Fig 10).

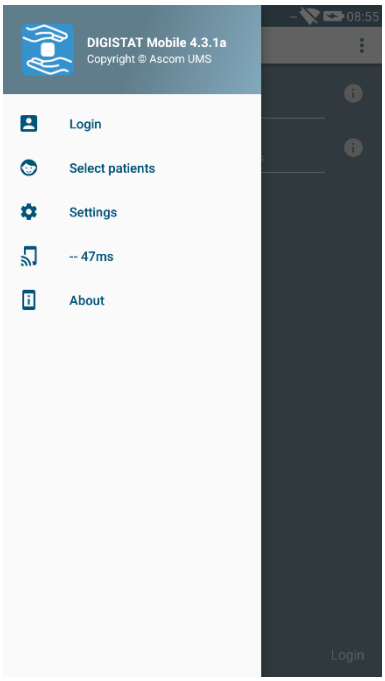

Fig 10

These are:

Login
Touch this option to access the login screen (described below - Fig 13).

Select Patients
Touch this option to access the Patients List (see paragraph 5.8).

Settings
Touch this option to access the Settings screen (see previous paragraph 5.2.2).

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 11 **A**) to display the licenses associated with the Product.

Fig 11

5.4 Login

To login to DIGISTAT® Mobile

- Touch **Login** on the lower-right corner of the “Applications list” screen (Fig 12 **A**)

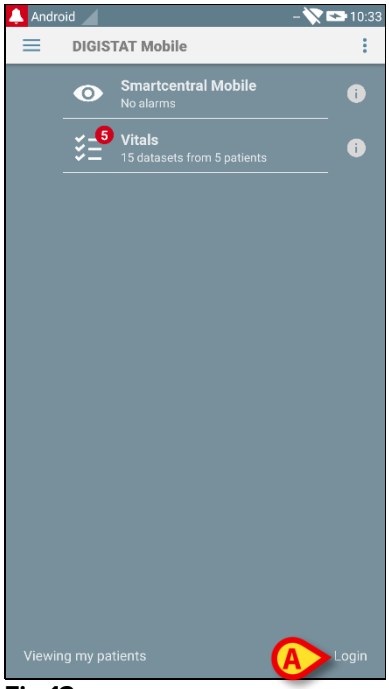

Fig 12

The following screen will be displayed (Fig 13)

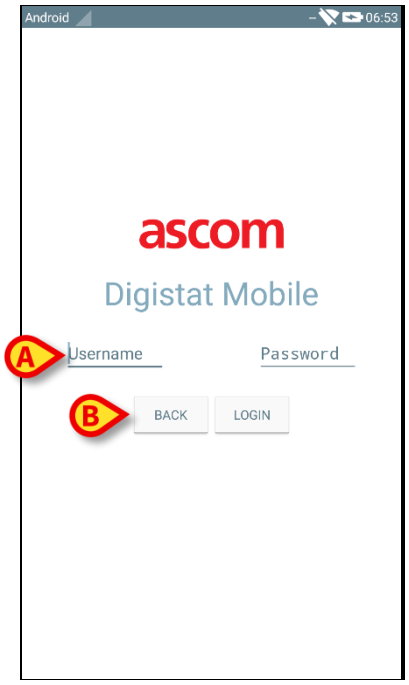

Fig 13

- Insert username and password (Fig 13 **A**).
- Touch the **Login** button (Fig 13 **B**)

The acronym indicating the logged user will then be displayed either on the "Applications list" screen (for Myco/UNITE version - Fig 14 **A**),

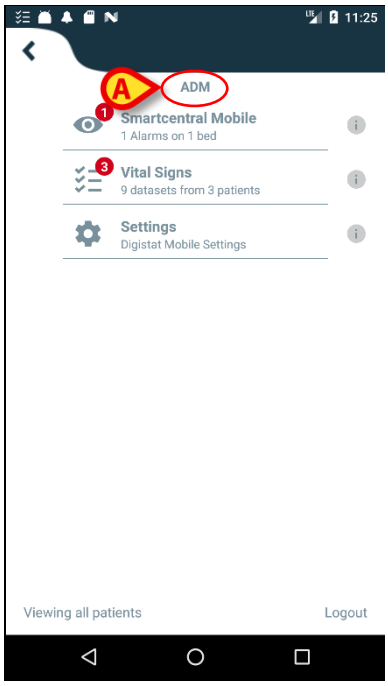

Fig 14

or on the upper notification bar (for other android handheld devices - Fig 15 **A**).

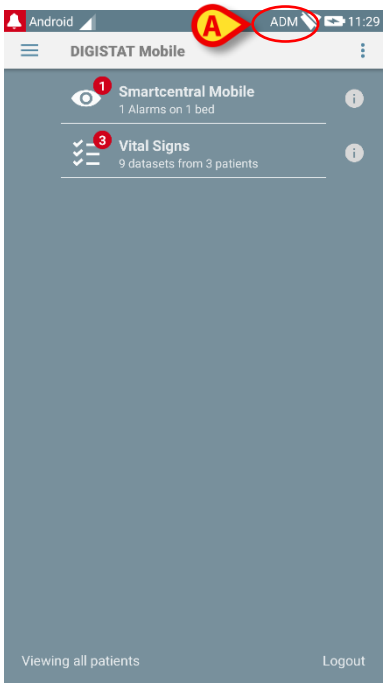

Fig 15

5.5 Upper notification bar

The upper notification bar (Fig 16 **A**) is always visible and displays general information.

Fig 16

The red bell icon placed on the top-left corner (only visible in non-Myco/UNITE devices - Fig 16 **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 16 **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 17 **A**).

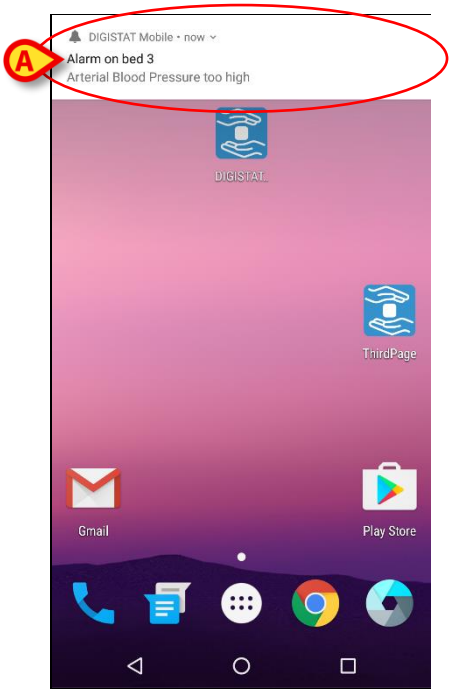

Fig 17

- Swipe the notification to make it disappear.

- Touch the notification to directly access the relevant module/patient (see an example in Fig 18, see paragraphs 6 and 7 for a description of the specific modules).

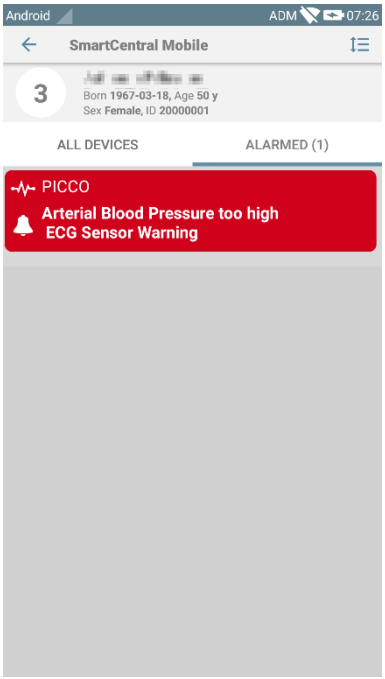

Fig 18

5.7 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 Smart Central Mobile application (Fig 19 **A**)

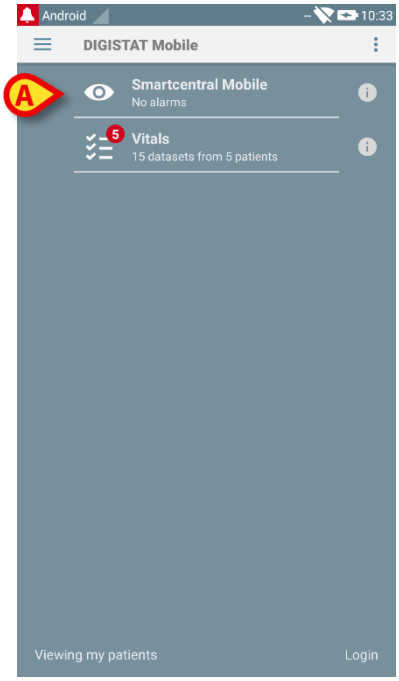

Fig 19

On any screen of the Smart Central Mobile Application,

- touch the ☰ icon on the top-left corner of the screen (Fig 20 **A**)

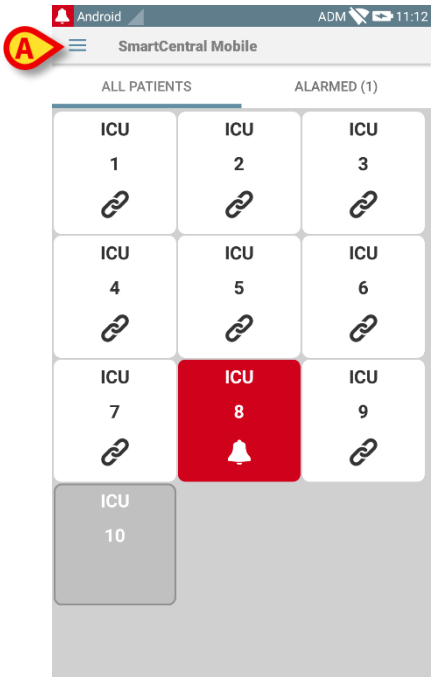

Fig 20

The following menu will be displayed (Fig 21).

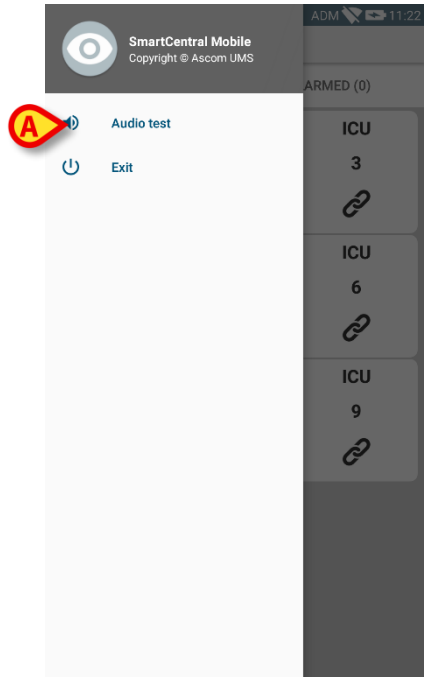

Fig 21

➢ Touch the **Audio test** option (Fig 21 **A**).

A test notification/sound will be this way provided (Fig 22 **A**).

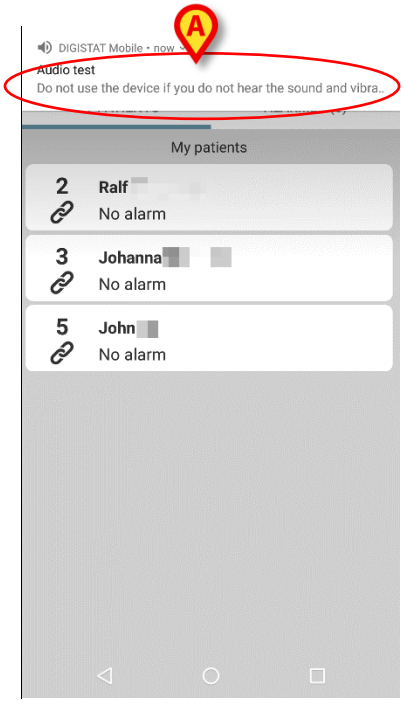

Fig 22

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

5.8 Patients search functionalities

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

To access the Patients List

- Touch the “mode” indication on the lower-left corner of the screen (Fig 23 **A** - this indication shows the current application mode, i.e. either “All Patients” or “My Patients” or “One Patient”, see paragraph 5.9 for a deeper explanation).

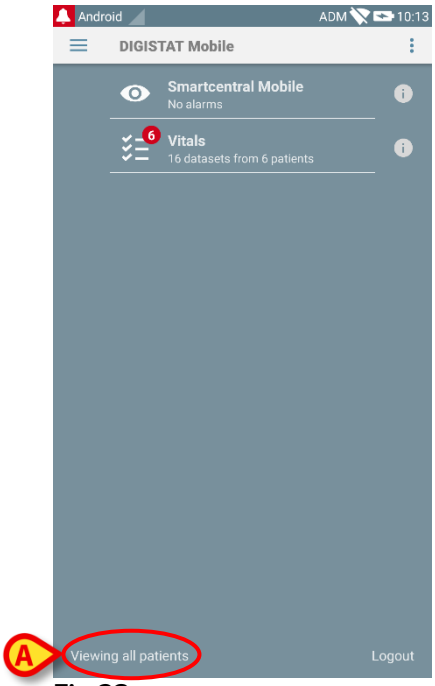

Fig 23

On the non-Myco/UNITE application the same screen can also be accessed touching the **Select Patients** option on the lateral menu (Fig 24 **A** - touch the ☰ icon on the top-left corner to open the menu).

Fig 24

In both cases, the following screen will open, containing the list of all the patients configured on the device domain (Fig 25).

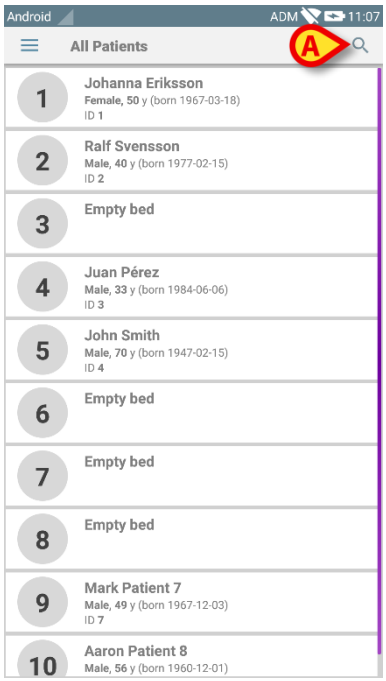

Fig 25

To access the search functionalities

- Touch the icon indicated in Fig 25 **A**.

The following screen will open (Fig 26).

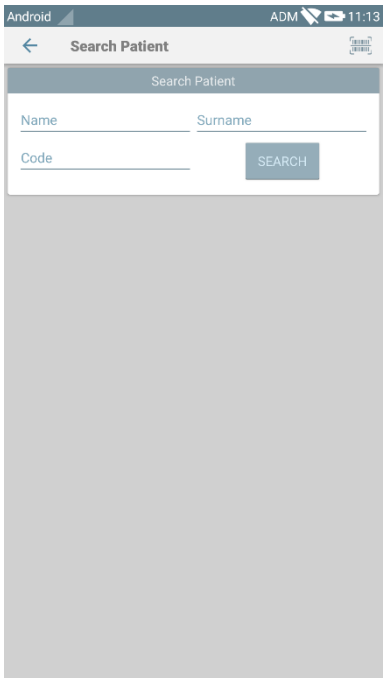

Fig 26

Three search options are available:

1 - textual search (see paragraph 5.8.1)
2 - barcode scan (see paragraph 5.8.2)
3 - NFC code scan (see paragraph 5.8.3)

5.8.1 Textual search

➢ insert patient data in the fields indicated in Fig 27 **A** (name, surname, code), then click the **Search** button (Fig 27 **B**). Partial information is allowed.

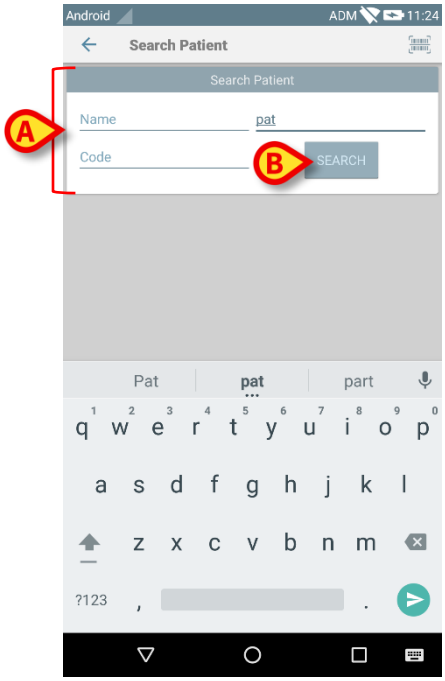

Fig 27

The list of patients whose data match those specified will be displayed (Fig 28).

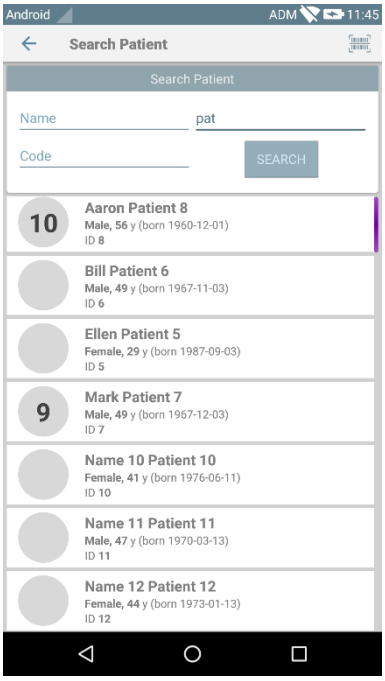

Fig 28

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 29).

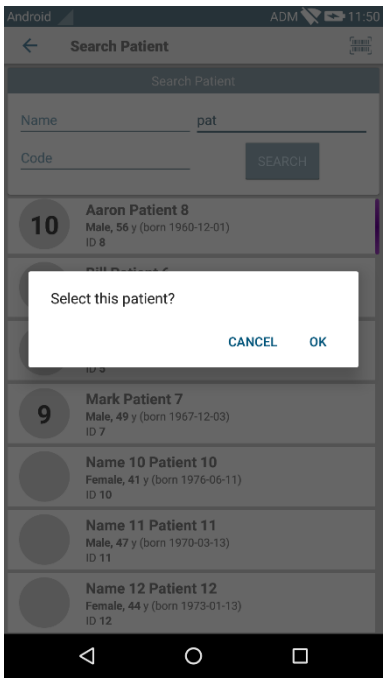

Fig 29

➢ Touch **Ok** to confirm.

The patient will be this way selected (Fig 30).

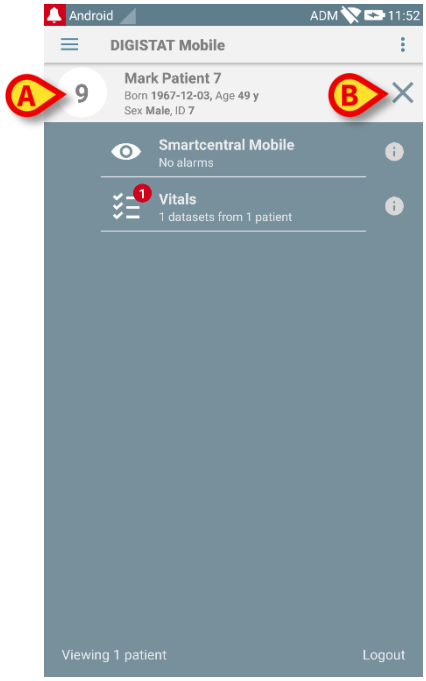

Fig 30

Patient data are on top of the page (Fig 30 **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 30 **B** to deselect the patient and turn to “All Patients” mode again.

5.8.2 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 5.8.

➢ Touch the  icon indicated in Fig 31 **A**.

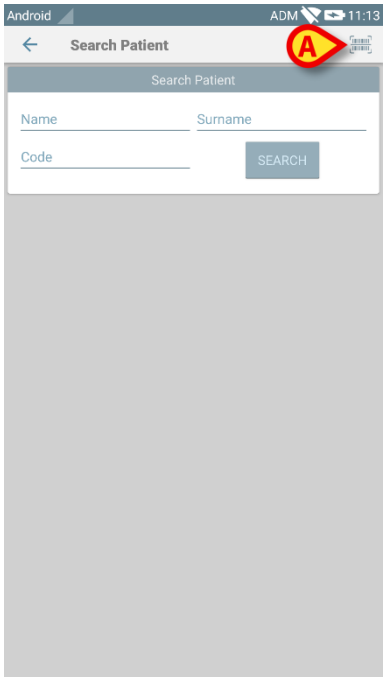

Fig 31

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 30 (example) will be displayed.

5.8.3 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 5.8.

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 30 will be displayed.

5.9 “My patients” mode

“My patients” mode makes it possible for a user to select one or more patients and create a “group” of patients who are under their charge.

“My patients” can be enabled or not by configuration and applies to the handheld device. So, there can be devices with “My patients” enabled and devices with “My patients” disabled.

This functionality does not depend on the module, i.e. once “My patients” is activated, all the modules will display information according to this mode.

Depending on the device configuration, if the “My patients” mode is activated, the following notifications can be displayed on the handheld device:

a) The notifications related to the patients selected as “My patients”;
b) The notifications related to the patients selected as “My patients” and those related to the patients that no one has explicitly taken in charge;
c) The notifications related to the patients selected as “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).

On the lower-left corner of the modules list screen, it is specified if the device is currently set on “My patients” or “All patients” (Fig 32 **A**).

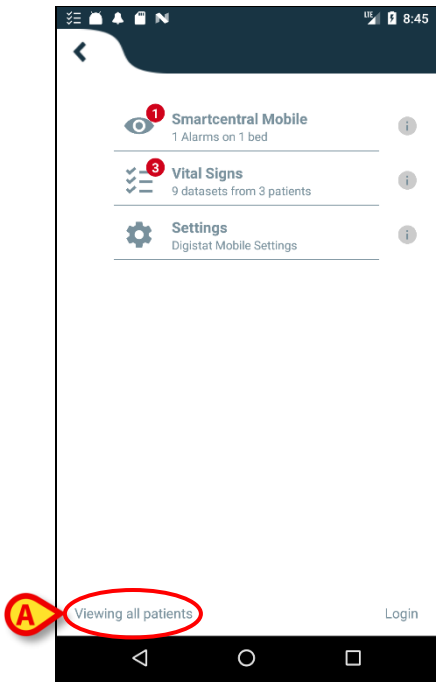

Fig 32

➢ Touch the indication (Fig 32 **A**) to display the managed patients list (Fig 33).

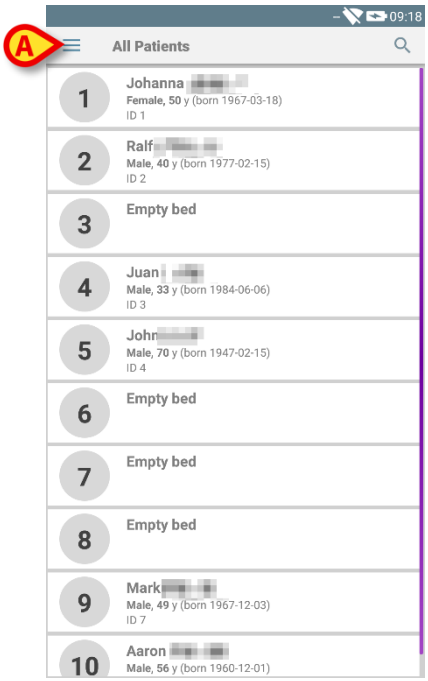

Fig 33

5.9.1 "My patients" activation

To activate "My patients"

- Touch the icon (Fig 33 **A**).

The following menu will open (Fig 34).

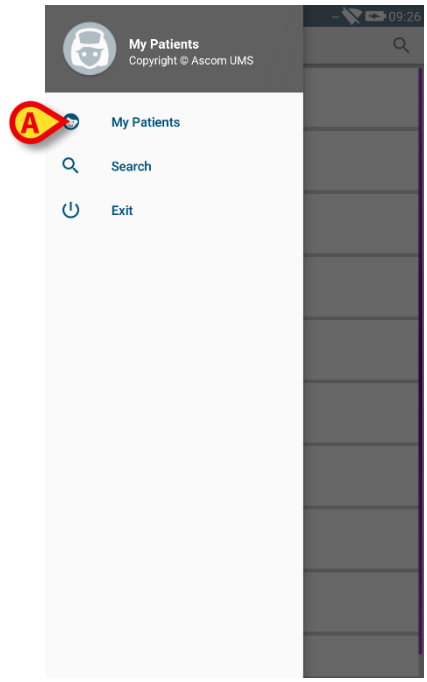

Fig 34

- Touch **My Patients** (Fig 34 **A**).

The device switches this way to “My patients” mode. “My patients” list will be displayed (Fig 35). In Fig 35 no patients is selected to be part of “My patients” list. See next paragraph for instructions on how to select “My patients”.

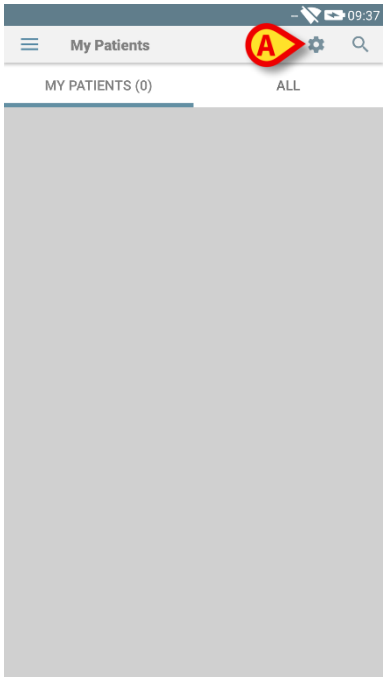

Fig 35

NOTE: The same procedure can be performed to switch back to “All patients”.

5.9.2 How to select “My patients”

To select the list of patients forming “My patients” list, on “My patients” list screen,

- touch the icon (Fig 35 **A**).

The following screen will be displayed (Fig 36 - “My patients setup”).

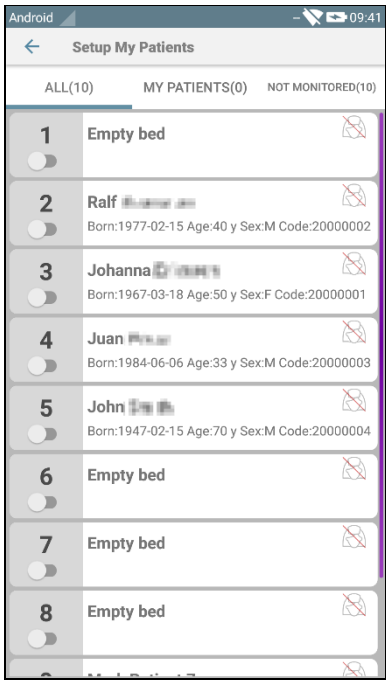

Fig 36

A patient can be selected/deselected by touching the corresponding “tile”. Each tile corresponds to a bed. In Fig 37 patients in bed 2, 3 and 5 are selected as “My patients”.

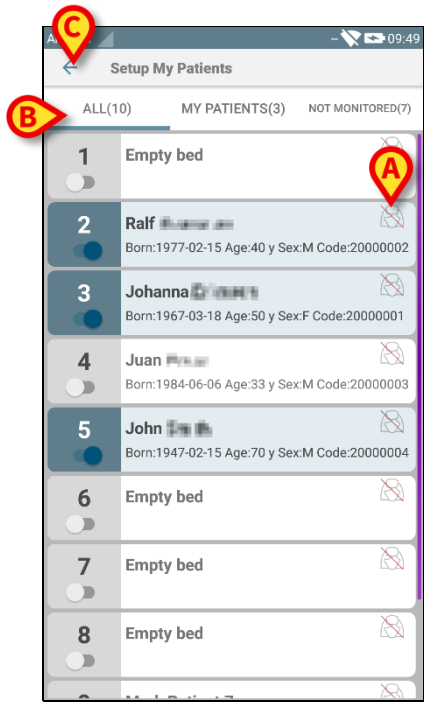

Fig 37

The icons on the right of the patient names (Fig 37 **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 37 **B** make it possible to display:

- all patients;
- only the selected patients (“My patients”);
- only the patients that are not monitored.

The icon indicated in Fig 37 **C** makes it possible to go back to “My Patients” list screen.

Use the filter indicated in Fig 38 **A** to display all patients again. The patients are now grouped as “My patients”, “Assigned to others” patients and “Unattended patients”.

NOTE: the number displayed alongside the filter refers to the total number of patients being part of “My patients” of any user.

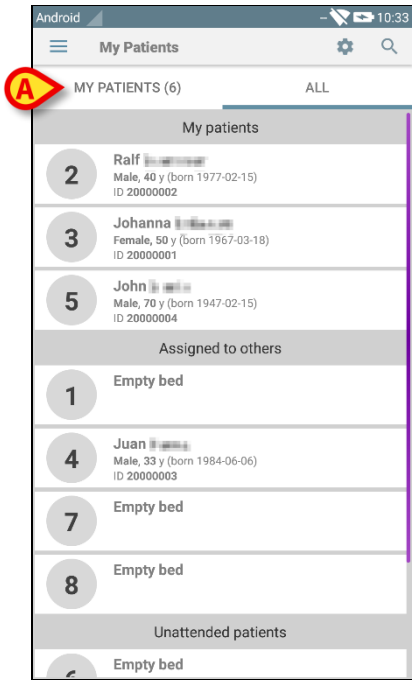

Fig 38

NOTE: When "My Patients" mode is active only the information relating to "My patients" is notified (can be alarms, patient info, procedural info or other, depending on the DIGISTAT® Mobile module/functionality selected).

5.10 Single Patient Selection

One single patient can be selected by touching the tile corresponding to his/her bed.

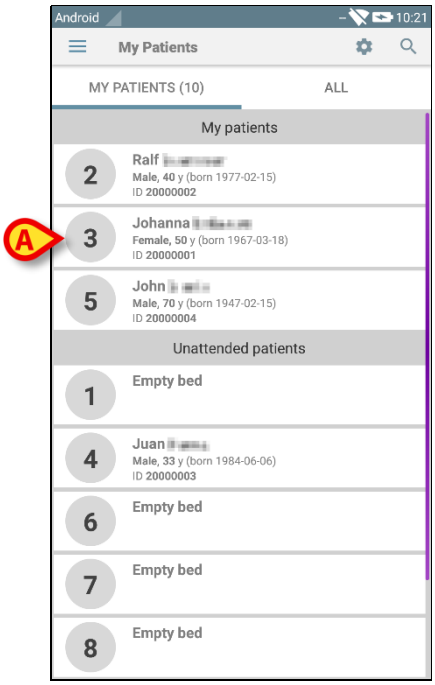

Fig 39

For instance, to select the patient on bed 3,

- Touch the tile indicated in Fig 39 **A**. User confirmation is required (Fig 40).

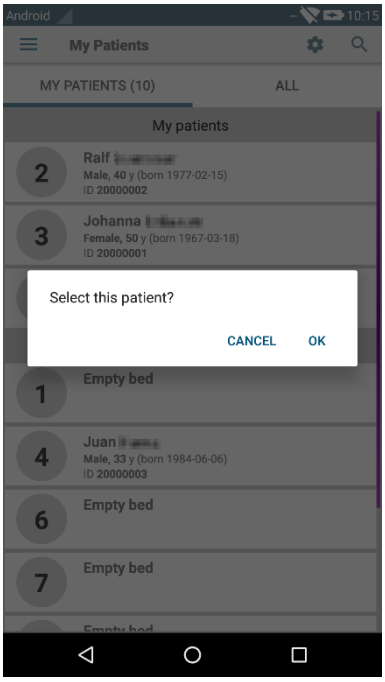

Fig 40

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

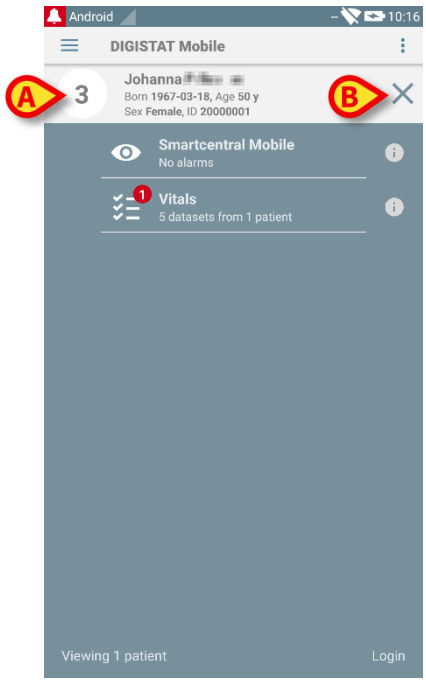

Fig 41

Patient data are on top of the page (Fig 41 **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 41 **B** to deselect the patient and turn to “All Patients” mode again.

6. DIGISTAT® “Vitals”

6.1 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.

6.2 Application start-up

To start the “Vitals” application

➢ Touch the corresponding row on the handheld device screen (Fig 42).

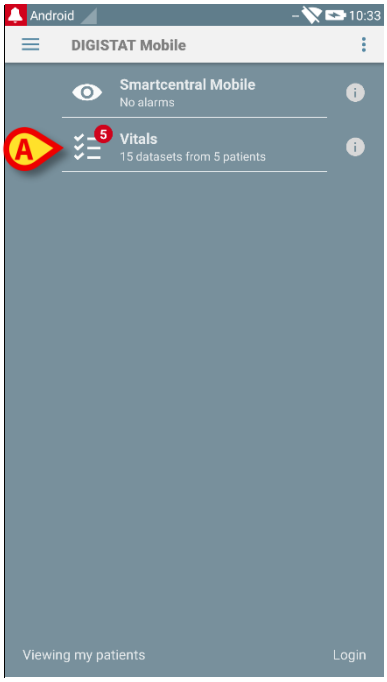

Fig 42

The “Vitals” screen, shown in Fig 43, will open.

Fig 43

6.3 Patients list

The “Vitals” patient list screen (Fig 44) 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.

Fig 44

The patient list screen is formed of a heading (Fig 44 **A**) and the patients list (Fig 44 **B**).

6.3.1 Patient list heading

Fig 45 shows the heading of the patient list screen.

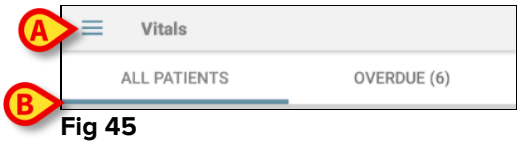

Fig 45

The menu indicated in Fig 45 **A** opens the **Exit** option (Fig 46).

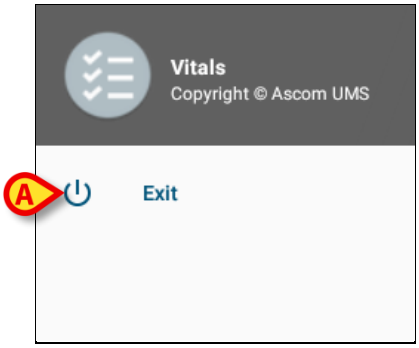

Fig 46

➢ Touch the **Exit** option (Fig 46 **A**) to quit the “Vitals” application.

The filter indicated in Fig 45 **B** 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**).

6.3.2 List of beds

Each bed is represented by a tile (Fig 47).

Fig 47

In the tile, the following information is displayed:

- bed number (Fig 47 **A**);
- number of notifications overdue (if any - Fig 47 **B**);
- name of patient on that bed (Fig 47 **C**);
- patient data (if available: sex, age, date of birth, patient ID - Fig 47 **D**).

➢ Touch one tile to access the list of datasets enabled for the corresponding patient (Fig 48).

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...

6.4 Datasets list

The datasets list screen is formed of two areas: a heading area (Fig 48 **A**) and the list of datasets (Fig 48 **B**).

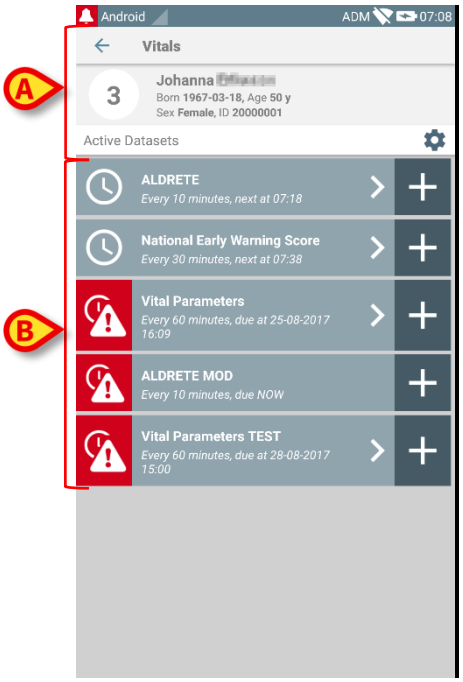

Fig 48

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 6.5 for the dataset configuration functionalities.

Fig 49 shows an example.

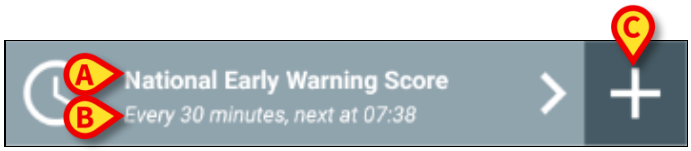

Fig 49

The dataset name is displayed inside the tile (“National Early Warning Score” - Fig 49 **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 49 **B**).

The + button (Fig 49 **C**) makes it possible to insert new data (see paragraph 6.4.1).

If the + button is not present on the tile it means that the dataset is not enabled (see paragraph 6.5 for more information). The tile is still displayed because past data exists for that dataset, which can be still viewed. See for instance Fig 50.

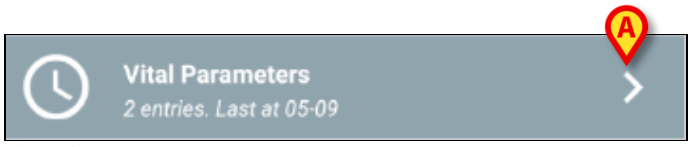

Fig 50

The arrow (Fig 50 **A**) makes it possible to display the past data. See for example Fig 51.

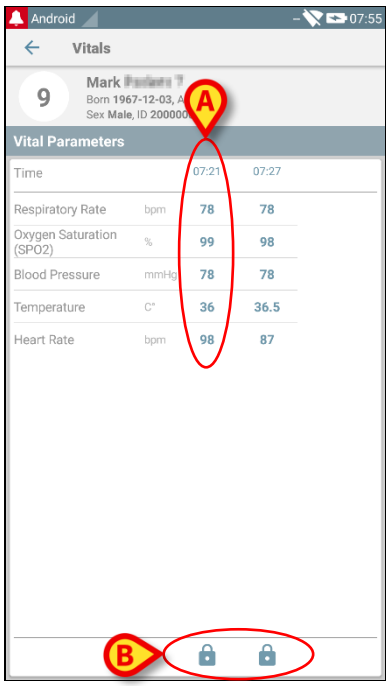

Fig 51

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 51 **A**.

The “lock” icon indicated in Fig 51 **B** means that the corresponding score cannot be edited. Otherwise a “pen” icon is displayed (see for instance Fig 57).

The datasets can be configured to provide a notification at scheduled times, as a reminder, when they should be acquired. See for instance Fig 52. The Aldrete score is here configured to be acquired every 10 minutes.

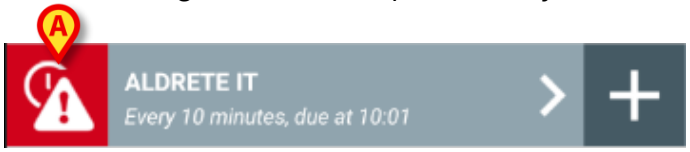

Fig 52

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 52 **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).

6.4.1 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 53).

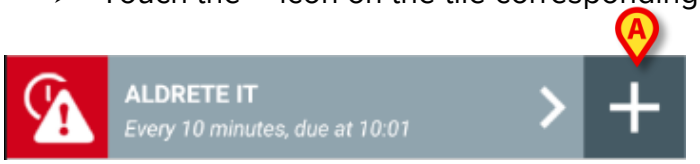

Fig 53

The data entry screen will be displayed.

NOTE: the data entry screen features depend on the kind of dataset selected. See Fig 54 for an example.

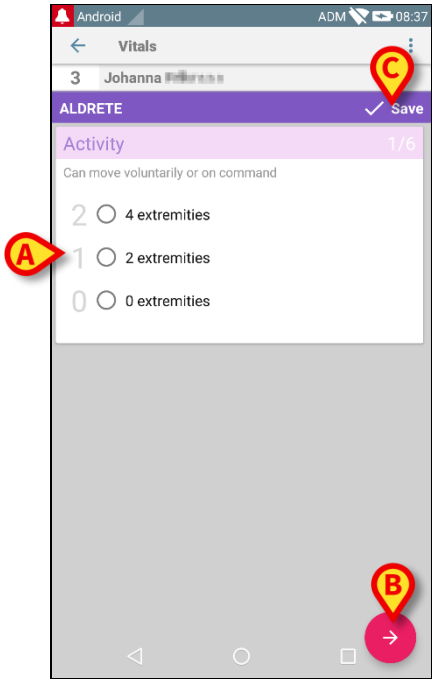

Fig 54

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 55 for another example.

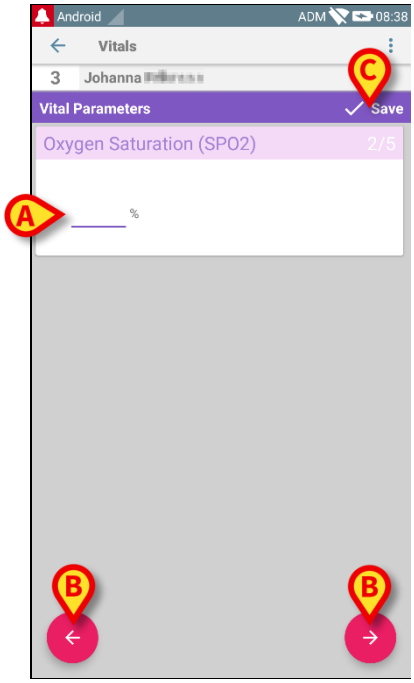

Fig 55

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 54 **A** and Fig 55 **A**).
- Move to next/previous screen using the arrows indicated in Fig 54 **B** and Fig 55 **B**.

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

- touch **Save** to save the dataset (Fig 54 **C** and Fig 55 **C**). The **Cancel** option closes the data entry screen.

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 56 **A**.

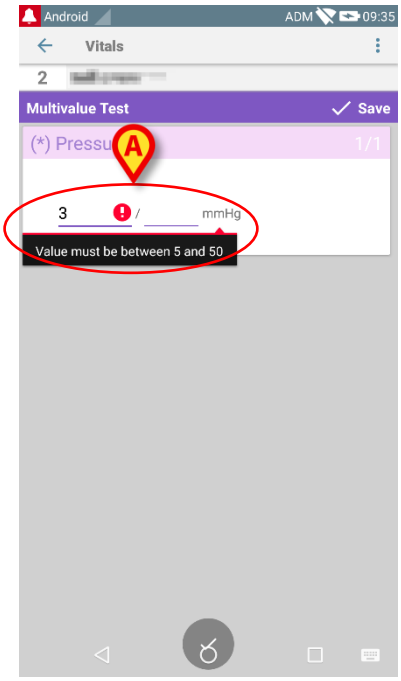

Fig 56

6.4.2 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 57 for an example.

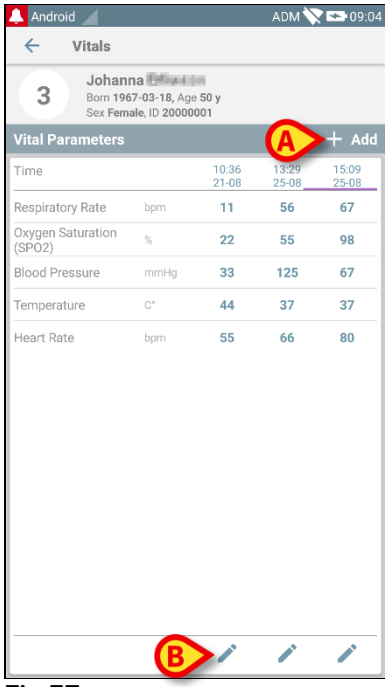

Fig 57

- On this screen, touch **Add** to add another set of data (Fig 57 **A**).
- Use the “Pen” icon to edit the data of an existing set (Fig 57 **B**).

6.4.3 How to edit an existing set of data

To edit an existing set of data, on the datasets list screen (Fig 58),

Fig 58

- Select the relevant dataset (Fig 58 **A**, for instance). The acquired datasets summary will open (Fig 59).

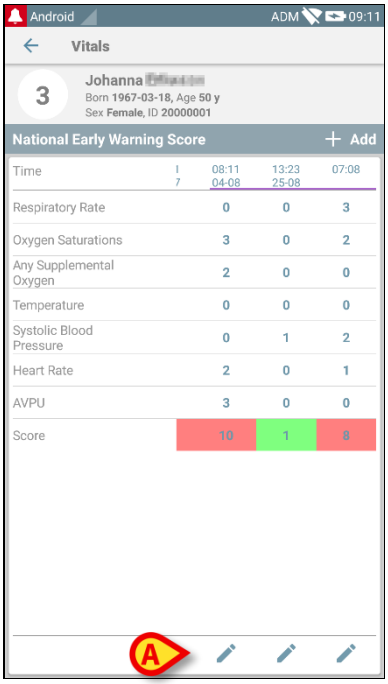

Fig 59

- Touch the “pen” icon corresponding to the set to be edited (Fig 59 **A**)

The data entry screen will open (Fig 60).

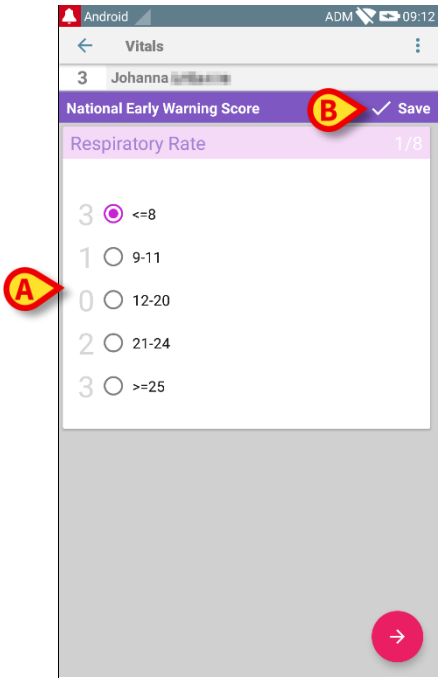

Fig 60

- Edit data (Fig 60 **A**).
- Touch **Save** (Fig 60 **B**).

The set is this way edited.

6.4.4 Pictures and audio acquisition

The “Vitals” application 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.

The following screen will open, making it possible to record an audio file (Fig 61).

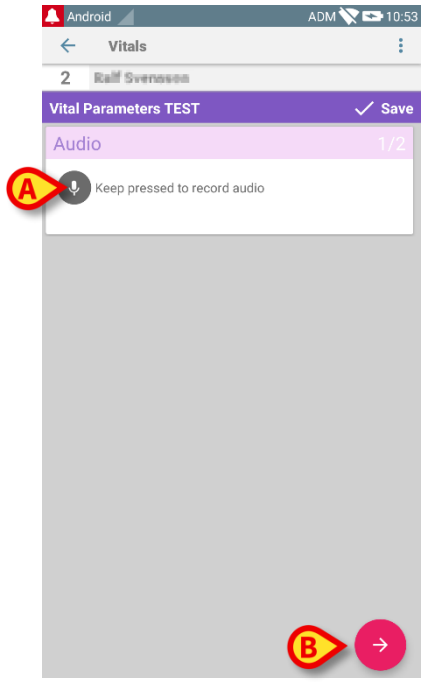

Fig 61

To record,

- keep pressed the button indicated in Fig 61 **A**.

The button will turn red while recording. Recording ends when the button is released. After recording the audio acquisition page is displayed (Fig 62). The icon indicated in Fig 62 **A** represents the recorded file.

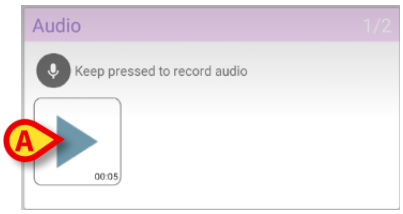

Fig 62

Multiple recordings are possible for a single dataset acquisition (Fig 63 **A**).

Fig 63

- 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 61 **B**).

The following screen will open (Fig 64)

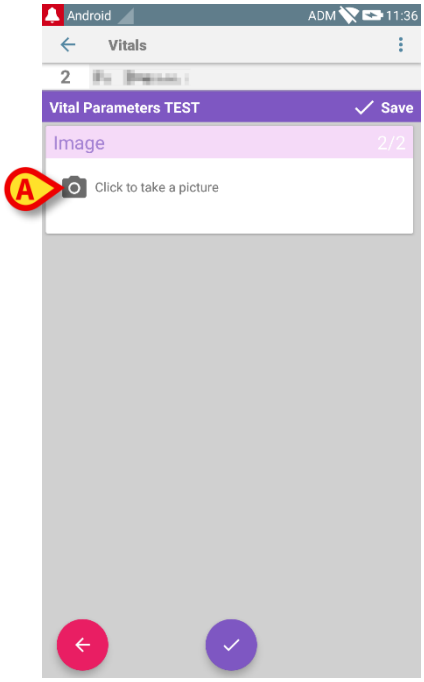

Fig 64

➢ Touch the icon indicated in Fig 64 **A** to activate the camera (Fig 65).

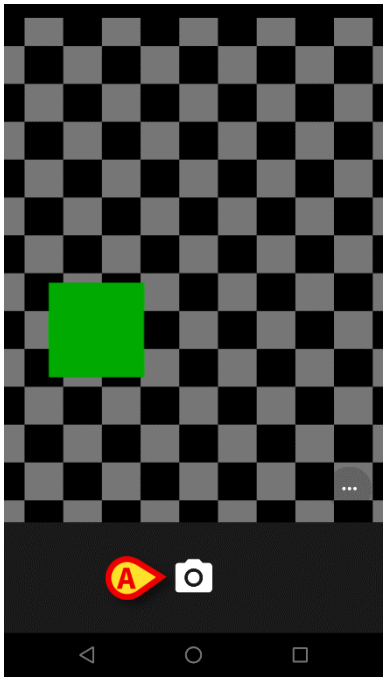

Fig 65

➢ Touch the icon to take the picture (Fig 65 **A**). A preview is displayed on screen (Fig 66).

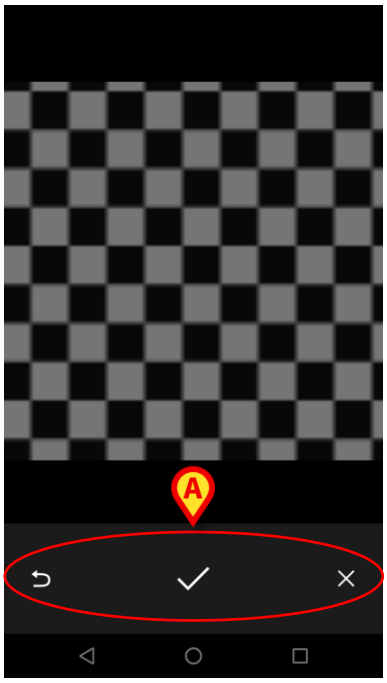

Fig 66

- Use the buttons indicated in Fig 66 **A** to:
  1. go back to the picture acquisition mode (Fig 65);
  2. keep the picture and go back to the photo acquisition page (Fig 64);
  3. discard the picture and go back to the photo acquisition page (Fig 64).

Once a picture is saved, a thumbnail is displayed on the photo acquisition page (Fig 67).

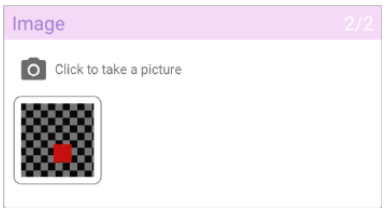

Fig 67

- 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 68),

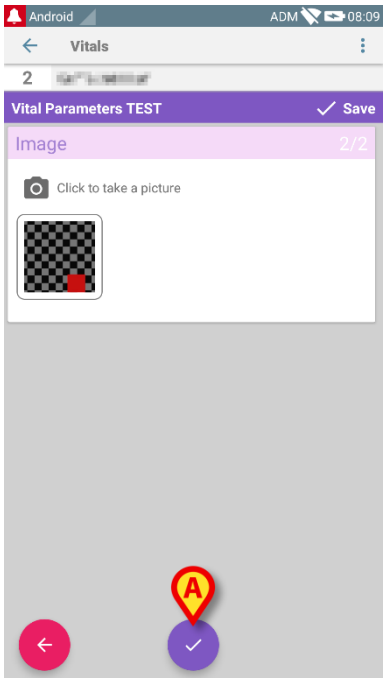

Fig 68

➢ Click the icon (Fig 68 **A**).

A summary screen is then displayed, listing all the acquired datasets (Fig 69).

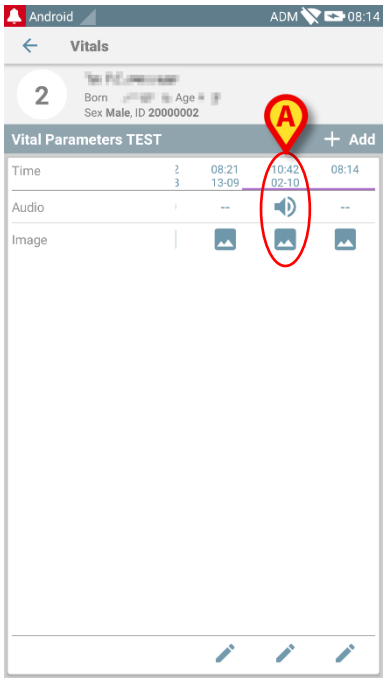

Fig 69

On this page, each column corresponds to a dataset (Fig 69 **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.

6.5 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 70),

➢ Touch the ⚙ icon (Fig 70 **A**).

Fig 70

The list of all the existing datasets (defined by configuration) will open (Fig 71).

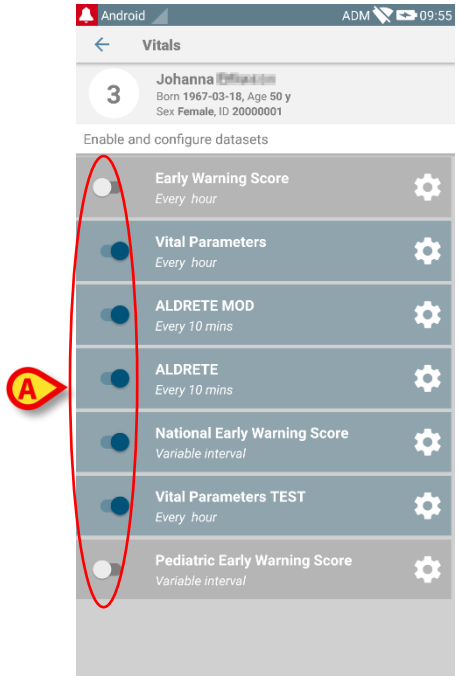

Fig 71

Use the switch on the left to enable/disable a dataset for the selected patient (Fig 71 **A**).
The switch is dark blue and positioned on the right when the dataset is enabled (Fig 72 **A**).

Fig 72

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

- Touch the  icon to configure the dataset (Fig 72 **B**).

The following screen will open (Fig 73).

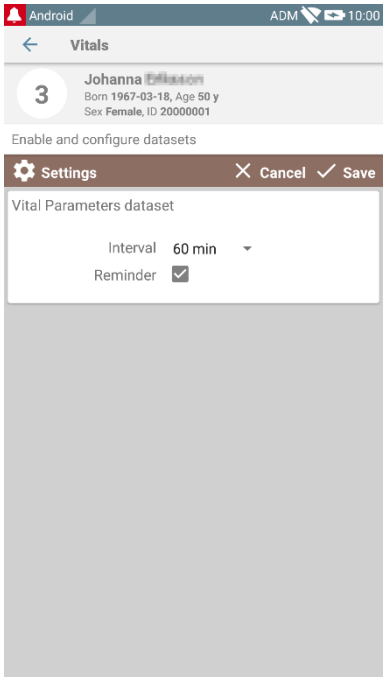

Fig 73

- Touch the “Interval” menu to decide the dataset timing (Fig 74).

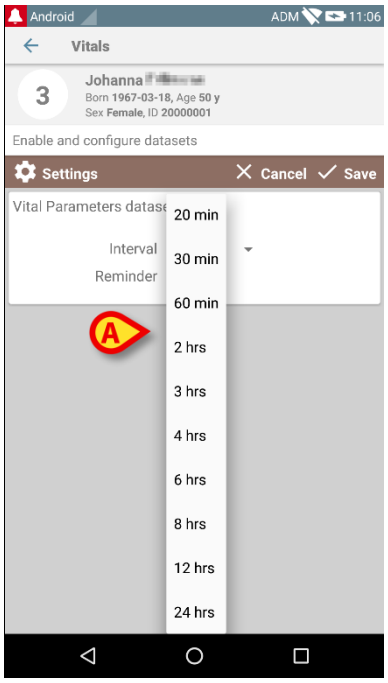

Fig 74

- Select the "Reminder" checkbox to get automatic reminders on when the datasets acquisitions are due (Fig 75 **A**).

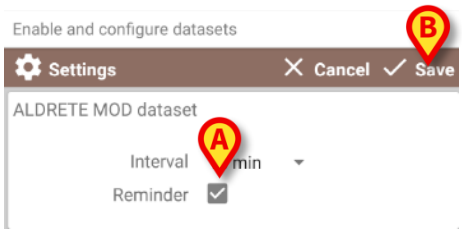

Fig 75

After configuring the dataset,

- touch the **Save** option to save the changes made (Fig 75 **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 76 **A**).

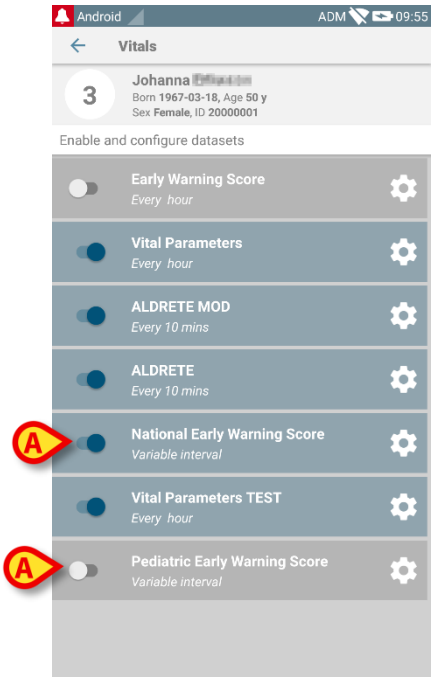
Android
ADM
09:55
Vitals
3
Johanna
Born 1967-03-18, Age 50 y
Sex Female, ID 20000001
Enable and configure datasets
Early Warning Score
Every hour
Vital Parameters
Every hour
ALDRETE MOD
Every 10 mins
ALDRETE
Every 10 mins
National Early Warning Score
Variable interval
Vital Parameters TEST
Every hour
Pediatric Early Warning Score
Variable interval
A
A

Fig 76

7. Smart Central Mobile

7.1 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.

7.2 Application start-up

To start the Smart Central Mobile application

➢ Touch the corresponding row on the handheld device screen.

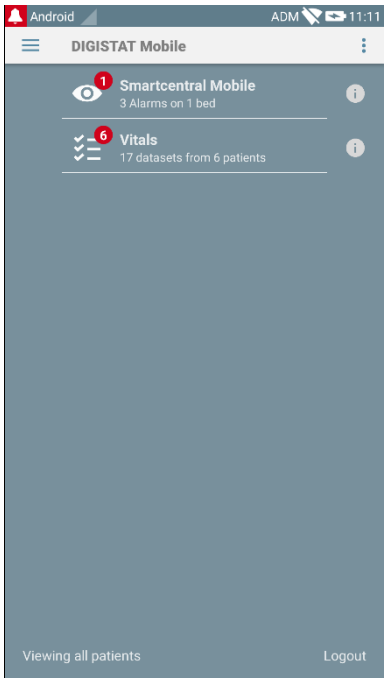

Fig 77

The Smart Central screen, shown in Fig 78, opens.

7.3 “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 (Fig 78).

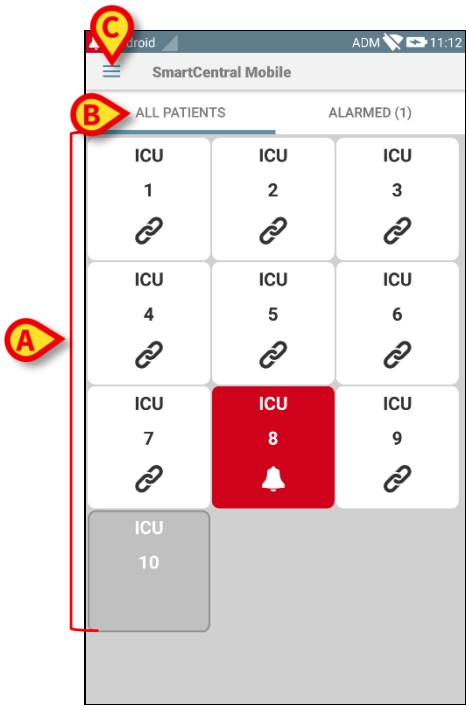

Fig 78

The numbered squares displayed on screen represent the beds configured in the handheld device (Fig 78 **A**). The squares visible on a single screen form the "domain" of beds covered by the handheld device. The "domain" is defined by configuration.

The number displayed inside the square indicates the bed number. On each square, 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.

You can use the filters indicated in Fig 78 **B** to display either all the configured beds or only the beds sending an alarm.

The  icon indicated in Fig 78 **C** opens the following menu (Fig 79).

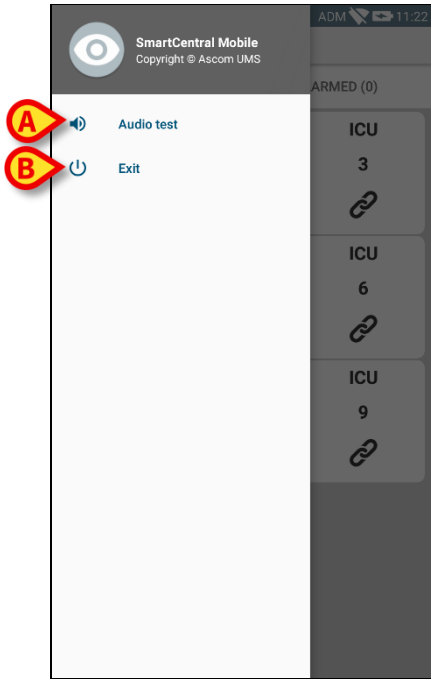

Fig 79

Audio test

Touch the **Audio Test** button (Fig 79 **A**) to test the sound-vibration associated to the notifications (see pargraph 5.7).

Exit

Touch the **Exit** button (Fig 79 **B**) to quit the application.

7.4 Medical devices list

Touch one of the squares on the “Central” screen to display the list of medical devices connected to the bed (Fig 80).

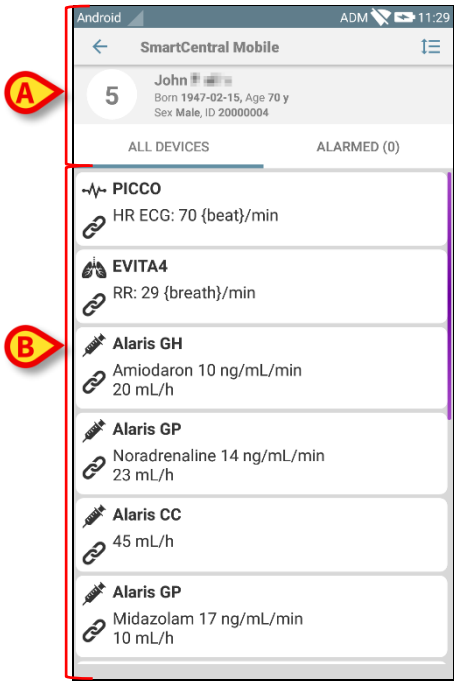

Fig 80

This screen is formed of two areas: a heading area (Fig 80 **A**) and the medical devices list (Fig 80 **B**).

7.4.1 Heading

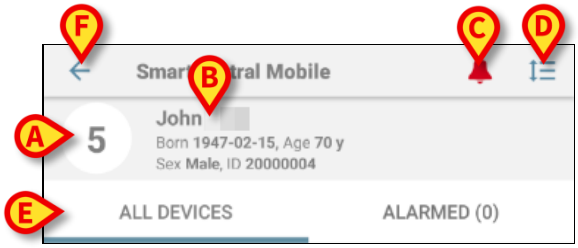

Fig 81

In the heading area (Fig 81) the following information and tools are available:

- Bed number (Fig 81 **A**).
- Patient data (Fig 81 **B**).
- The red bell icon (Fig 81 **C**) indicates that there is at least one medical device alarmed on one of the other beds (those not currently displayed).
- Use the icon indicated in Fig 81 **D** to enlarge the device-areas and display more information for each connected medical device (Fig 82). The type of information displayed depends on the configuration and the specific device.

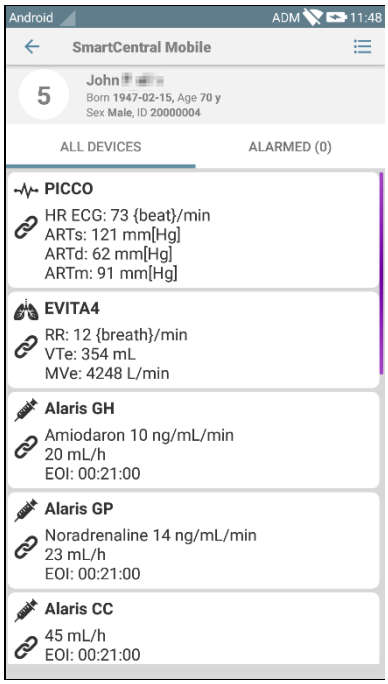

Fig 82

Touch the icon (Fig 81 **D**) again to go back to compact display mode.

Use the filters indicated in Fig 81 **E** to display either all the connected medical devices or only the ones providing notifications.

Use the back-arrow button (Fig 81 **F**) to go back to the “Central” screen.

7.4.2 Devices list

On the lower part of the “Bed” screen the individual medical devices are represented as shown in Fig 83:

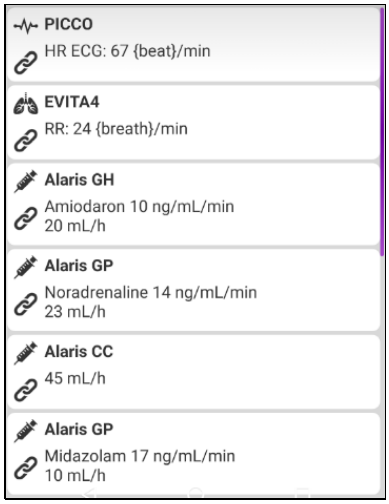

Fig 83

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 facility 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.

7.5 Alarms history

Each “card” can be touched to access the list of all the alarms provided by the medical device (Fig 84).

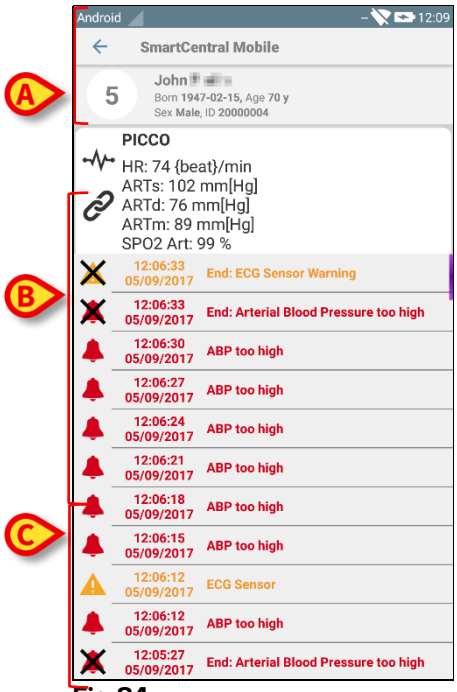

Fig 84

This screen is formed of three areas.

Patient data (Fig 84 **A**).
Medical device current data. The data displayed on this “card”, again depend on the device type and configuration (Fig 84 **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 84 **C**). For each alarm are displayed the beginning time and end time (black cross on the icon).

8. 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

9. 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.