mindray

healthcare within reach

Mindray General Data Protection Regulation (GDPR) Compliance White Paper

May 2018

Contents

Introduction

As a leading global developer, manufacturer, and supplier of medical devices, Mindray is dedicated to deliver high-quality, richly featured medical products making healthcare more accessible and affordable around the world. Since founded in 1991, Mindray has been striving not only to provide medical devices and industry solutions, but also practice corporate value into every aspect of company. To better serve clients, Mindray follows the most stringent international and FDA manufacturing and quality control standards in each of its state-of-the art manufacturing facilities, ensuring efficiency and traceability throughout the entire process.

This White Paper aims to provide our clients and stakeholders information to better understand the Mindray privacy policy. Specifically, this White Paper describes how Mindray implements its privacy policy to collect, store, transfer and delete data in the process of product design, manufacture, sales and use. With the approaching effective date of General Data Protection Regulation (GDPR) of European Union, Mindray has been taking effective actions to comply with GDPR compliance frameworks. Mindray is a leading practitioner at the forefront of industry compliance practices all along.

In this White Paper, it will help you to understand:

- Mindray's overall privacy protection policy, including guiding principles adopted by Mindray Headquarters and its subsidiaries;
- Mindray GDPR compliance programme illustrating the corporate governance and internal controls with regards to the considerations of privacy protection;
- The mechanism of Mindray's products, including PMLS, IVD, MIS, on how to collect, store, transfer and delete data.

Disclaimer:

Part 1

About Mindray

Our Company

Mindray is a leading global designer, developer, and manufacturer of medical devices and solutions, dedicated to making better healthcare more accessible to humanity. Since its foundation in 1991, Mindray has been exclusively focused on the medical industry in the fields of Patient Monitoring & Life Support, In-Vitro Diagnostics, and Medical Imaging. Mindray strives to be innovative, accessible, localized, and responsible. Mindray's insightful, human-centric research creates solutions that are designed with accessibility in mind, resulting in ease-of-use solutions in any solution.

With corporate headquarters located in Shenzhen, China, and 42 international subsidiaries with branch offices in 32 countries, Mindray has approximately 7,500 employees worldwide. Eight global R&D centers and an industry leading investment of 10% of annual revenue into research and development further demonstrates Mindray's commitment to innovation and advancing technology in a global market.

Our Vision

Better healthcare for all.

Our Mission

Advance medical technologies to make healthcare more accessible.

Our Commitment

Mindray is strongly committed to protecting the privacy of personal data that they maintain about our clients, employees and other individuals. As part of this commitment to privacy, Mindray regularly reviews its data protection practices to comply with applicable laws, industry standards and best practices. In preparation for May 25, 2018, when the European Union's General Data Protection Regulation (GDPR) will be enforced, and because of other territorial regulations impacting privacy, a GDPR compliance programme has been initiated to provide on a basis for, and a consistent approach to, data protection compliance across the Mindray Headquarters and European subsidiaries. All related subsidiaries are now in the process of implementing the requirements of GDPR, building on existing confidentiality and security processes and standards. The new GDPR compliance programme are extensive and cover multiple functional areas and aspects of our business, all in pursuit of accountability and transparency in how Mindray collects, process, protects and disposes of personal data. Despite that the present GDPR compliance program will finish in May 2018, Mindray's continuous improvement in this area is a long lasting mission.

Part 2

GDPR briefing

GDPR Overview: A Regulatory Change

As is becoming effective in May 25, 2018, General Data Protection Regulation (GDPR) will deal personal data and intend to give individuals more control over their data. The new GDPR will impose a regulatory framework on Europe and the wider world for the processing of personal data relating to an individual in the EU. Compared to the prior regulation, GDPR shifts the focus from organisational responsibilities to the rights of individuals by strengthening their ability to know where it is, how it is being used, to make sure it is correct, to have it deleted or transferred, and to object to it being used.

This regulation shift changes the way organisations or companies to collect and process data, especially some categories of personal data (health, ethnicity, religion, biometrics, sexual orientation, etc.) having even more demanding conditions. Accordingly, there is a new requirement for organisations or companies to document their processing activities of how they are protecting personal data and using lawfully, fairly and transparently.

Is Mindray well prepared for GDPR?

Mindray is working closely with its staff, clients and third parties about GDPR compliance programme between Headquarters and Europe. According to GDPR requirements, Mindray implements reasonable and appropriate organisational and technical measures to ensure that the nature, scope, context and purpose of our products are under regulation framework.

Mindra practices Privac b Design, and our products have been designed with the considerations relevant to GDPR requirements from the beginning of the project and throughout the entire lifec cle.

Part 3

How we protect our clients information

Mindray General Data Protection Regulation (GDPR) Programme

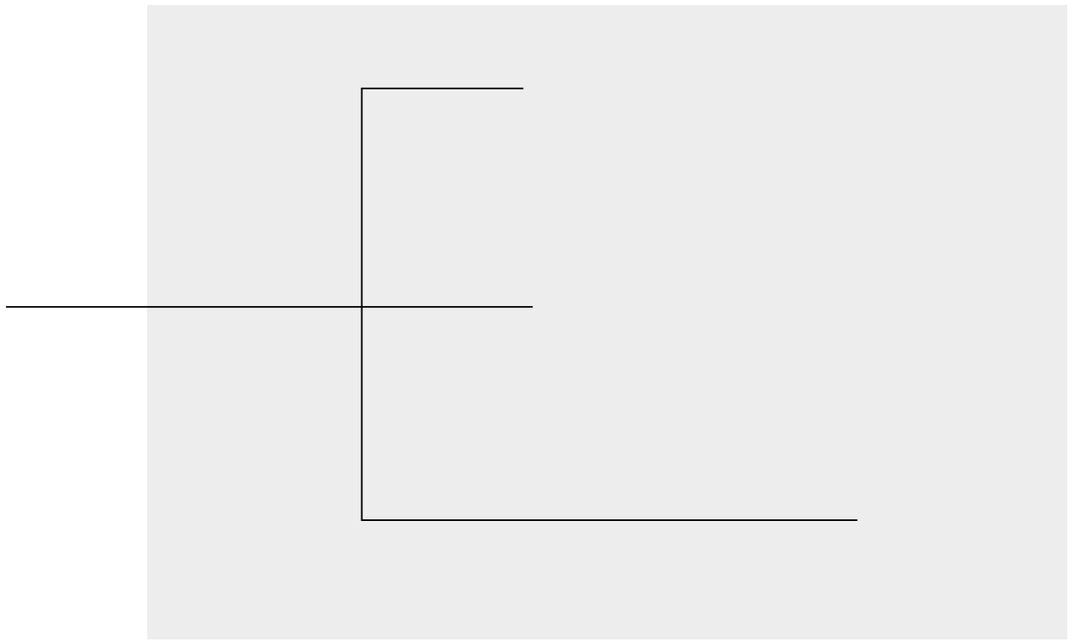
Given Mindray's global footprint and expansive business model, our firms and subsidiaries sit at the convergence of market demands and regulatory forces related to data, especially the GDPR which is coming into effect on May 2018.

Mindray intends to build the programme on the existing Information Protection Standard and is designed to achieve a level of enhanced baseline uniformity across the globe, informed chiefly by the prevailing and dominant legal requirements, emerging client demands, and the need to facilitate the realisation of Mindray's commercial targets.

To better meet GDPR compliance requirements and protect customer's privacy, Mindray has launched a GDPR compliance programme positively and proactively. In accordance to GDPR compliance core areas, Mindray will demonstrate the security of the data processing and compliance with the GDPR on a continual basis, by implementing and regularly reviewing robust technical and organisational measures, as well as compliance policies in this White Paper.

Mindray GDPR Compliance Programme Organisation Chart

In accordance with the requirement of GDPR, Mindray improves and develops the corporate governance structure. The compliance governance structure is a modernised, accountability-based framework that facilitates internal control and response to data breach issues. The organisational structure should be clear and reliable so that every relevant department is involve in data protection activities. From top to bottom, the GDPR compliance organisational structure is as shown below.



The GDPR compliance organisational structure has been divided into three core responsibility areas and are as follows:

- The GDPR Compliance Senior Management provides compliance strategic vision and plan, as well as performs tactical and strategic management of the GDPR Programme;
- The Data Protection Officer (DPO) is in charge of daily compliance operation and coordinates the operation of internal departments, including subsidiaries of Europe;
- The internal departments within the company perform the day-to-day GDPR operational activities.

The Data Protection Officer (DPO) is the core role of the GDPR compliance programme. This role is responsible for the day-to-day operations of the compliance activities. The DPO is involved, properly and in a timely manner, in all issues which relate to the protection of personal data. The responsibilities of DPO are including:

- Managing compliance violations;
- Working with relevant business units to enhance their awareness and propose corrective measures;
- Following up with the updates from regulators and notifying the relevant parties;
- Determining the adequacy of the inclusivity of data protection clauses in contracts;
- Reviewing and commenting on the data protections clauses from client.

Mindray hopes to protect client's privacy through practical and effective actions. This will benefit clients:

- Using information in a way that people would reasonably expect. This may involve undertaking research to understand people's expectations about how their data will be used;
- Thinking about the impact of your processing. Will it have unjustified adverse effects on them? and;
- Being transparent and ensuring that people know how their information will be used. This means providing privacy notices or making them available, using the most appropriate mechanisms.

2. Data Lifecycle Management

Data Lifecycle Management (DLM) is a policy-based approach to managing the flow of an information system's data throughout its life cycle: from creation and initial storage to the time when it becomes obsolete and is deleted.

DLM includes every phase of a "record" from its beginning to its end. To some extent, DLM means a corporate management control of all informational assets. During its existence, information can become a record by being identified as documenting a business transaction or as satisfying a business need. In this sense, DLM has been part of the overall approach of enterprise content management.

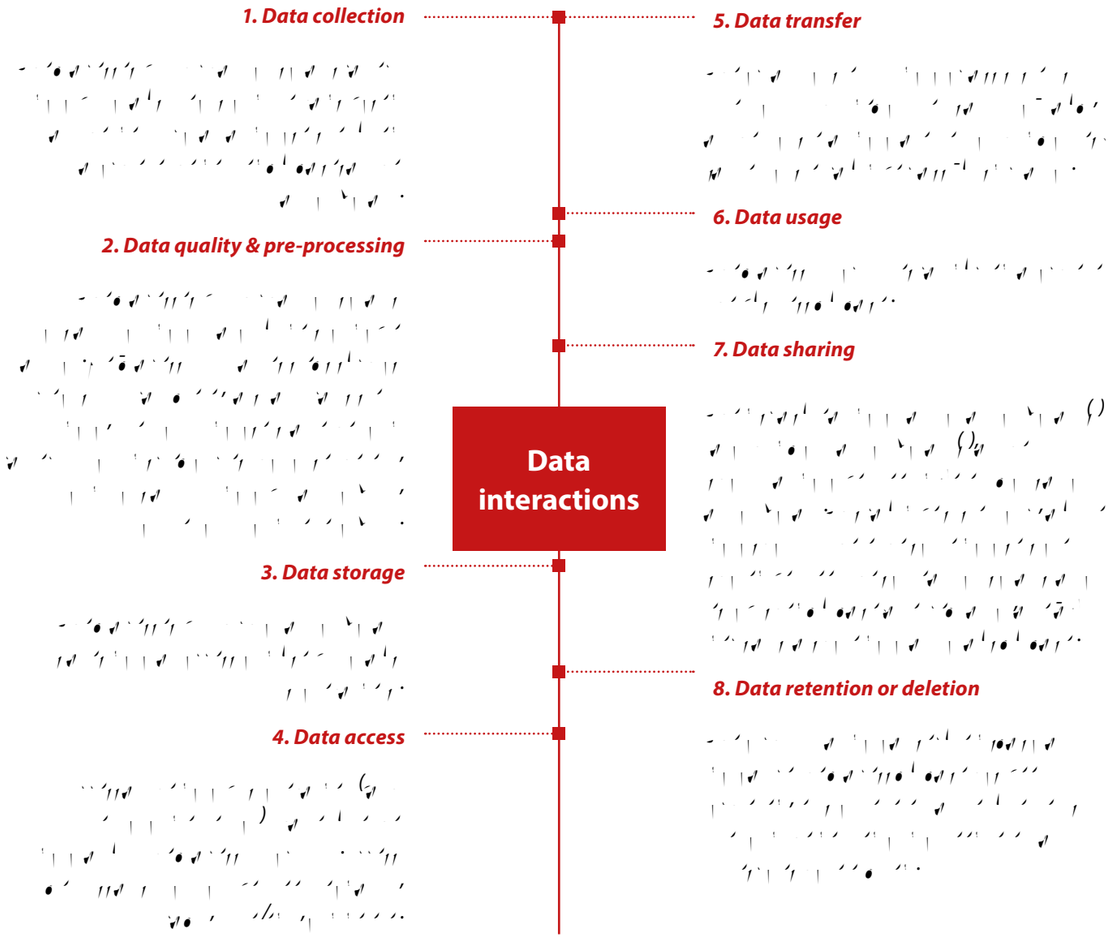
DLM, as a new management method, has the following on offer in order to promote business transformation and revolution:

- Fully incorporate the technical aspects, performance and cost along with the schedule requirements into a holistic work pack with complete traceability to client demands all through the lifecycle;
- Plan as well as implement the plan with complete configuration management of designs and documents including the program management artifacts;
- Seamlessly and securely collaborate and contribute to the existing knowledge base and share best practices across the total value chain;
- Have a unique master single source of truth of consolidated data with which are used to define most complex medical devices and platforms of Mindray and integrate a virtual global network of product developers, designers, production specialists, manufacturing engineers and service/ support teams.

Moreover, due to the huge value of personal data and sever consequence of data leakage, major countries and regions worldwide have accelerated the legislative process to protect personal data and privacy. General Data Protection Regulation (GDPR) from European Union is a representative example.

Country/Region	Law/Regulation	Issue Date
United States	Health Insurance Portability and Accountability Act of 1996 (HIPAA)	1996
European Union	General Data Protection Regulation (GDPR)	2016
China	People's Republic of China Network Security Law	2017
Hong Kong SAR of PRC	Personal Data (Privacy) Ordinance	1996
Australia	Privacy Act 1988	1988
New Zealand	Privacy Act 1993	1993
Japan	Personal Information Protection Law	2005
Republic of Korea	Personal Information Protection Law	2011
Republic of Singapore	Personal Information Protection Law	2013

What is more important is an understanding of what the GDPR is really seeking to achieve, what the real risk issues are; how to prioritise compliance activity; and how to build appropriate structures for compliance. The GDPR is seeking to (1) put people back in control of their personal data and (2) improve the protections for personal data at the entity's side. Thus, the GDPR raises countless issues in operating environments such as Mindray. Under these circumstances, Mindray adjusts corporate governance and refines internal control policies in time to meet GDPR requirements.



According to GDPR, Mindray divides data lifecycle into several phases and develops critical controls at each phase. Mindray designs each critical control in accordance with GDPR requirements and company's business practice. Here takes data collection, data storage, data transfer phases as typical examples as shown in the table below:

Data Lifecycle Phase	Mindray's Efforts	GDPR Core Requirements
1. Data Collection	Mindray will clarify responsibilities and obligations about personal information protection with the cooperative medical institutions in signed contract;	Consent
	Mindray will ensure that clinical trial participants or product users have signed informed consent form with medical institutions;	
	Mindray will follow the process control requirements of Privacy by Design in the implementation of the software development and testing phase;	Privacy by Design
	Mindray will ensure only really necessary personal identifiable information (PII) and protected health information (PHI) collected.	Data Concerning Health Scope
2. Data Storage	Mindray will ensure collected data is stored securely. Both logical and physical security control measures are deployed under implementation;	Data Protection
	Mindray will take appropriate measures considering (1) the state of the art (2) the cost of implementation (3) the nature, scope, context and purposes of the processing and (4) the risk posed to data subjects;	Data Protection by Design
	Mindray will ensure that, by default, collected data isn't made available to an indefinite number of people without some action by the data subject;	Data Protection by Default
	Mindray will ensure collected data will be stored under the premise (1) as required by professional standards or policies (2) as required or permitted by law.	Lawful Retention of Personal Data

Data Lifecycle Phase	Mindray's Efforts	GDPR Core Requirements
3. Data Transfer	Mindray will ensure that the contract signed between the medical institutions and test subject includes the clause fully informs the test subject of cross-border transfer;	Consent
	Mindray will ensure that there is a liability clause of cross-border transfer between medical institutions (data senders) and Mindray headquarters (data receivers);	
	Mindray will ensure the cross-border transfer of data security and compliance;	Data Protection
	Mindray will ensure only the necessary data is transferred to comply with the regulation.	Privacy by Design

3. Privacy Notice

Mindray respects and values user privacy. Accordingly, Mindray has drafted a detailed privacy notice to help user understand our privacy policy and responsibility. Mindray understands that users trust us with their data. Hence, Mindray takes this trust seriously and is committed to respecting each user's privacy and protecting the personal data we handle. There are two approaches to help users to better know the privacy policy of Mindray. The first one is the Privacy Notice link at the bottom of our website. The other one is in the email that is sent to our users. They can easily find the Privacy Notice link in the email and get more information from the external page. The Mindray Privacy Notice informs our users about the following topics regarding their privacy:

- What personal data will Mindray collect and process?
- How Mindray use your personal data?
- How does Mindray protect your personal data?
- With whom Mindray shares your personal data?
- How Mindray respects your privacy in marketing activities?
- How to request access to your personal data?
- How to contact Mindray?

4. Decontamination Process

Mindray has designed a decontamination process for demo machines to ensure all personal data has been wiped out prior to next use. The workflow regulates detailed procedures when the demo machines are returning. There will be a decontamination card attached to a demo machine after all workflow is finished. This card is used for declaration and traceable purposes.

Part 4

How our products are designed to meet the requirements of GDPR

Mindray's comprehensive product portfolio, built on a foundation of a thorough understanding of our customer's needs, enables us to offer the right solution for a number of different care environments, including pre-hospital care, emergency care, perioperative care and intensive care. Mindray's extensive global R&D network utilises cutting-edge technology and translates it into customised healthcare solutions. Mindray's integrated innovation platform combined with commitment to product and service quality has positioned Mindray as one of the leading clinical solution providers, making better healthcare more accessible to humanity.

While Mindray products insist on the pursuit of quality and technology, we are strongly committed to protecting user personal information as well. As part of our efforts to enhance personal data protection practices and comply with evolving regulations around data privacy, we have robust and practical measures at the product level to provide our users and clients in compliance with laws and regulations, e.g. GDPR.

With the approaching enforcement date of General Data Protection Regulation (GDPR), Mindray has taken reasonable and necessary measures to safeguard all the products that are in compliance. Mindray's products offer many built-in functionalities that help users lower the possibility of data breach incidents and respond to a data subject's requests.

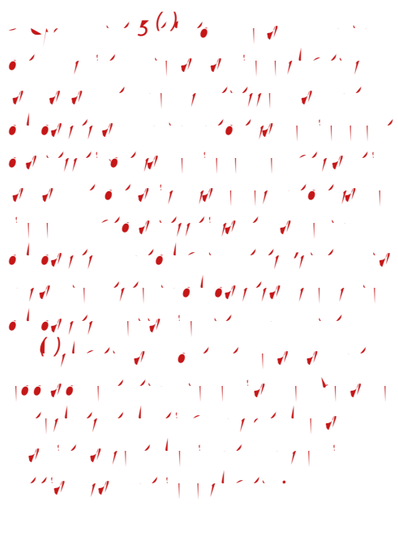
The following descriptions are specifically illustrating our products' ability to ensure ongoing confidentiality, integrity, availability under the framework of GDPR. The tables below are an overview to show how our products are meeting the principles and data subject rights of GDPR.

2. Data Minimisation

Mindray ensures that personal data is collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Mindray will not collect extra personal data that is irrelevant with product use purpose. For example, Mindray's IVD products will collect the following information for medical service:

- Personally Identifiable Information
  - Patient Name
  - Gender
  - Age
- Medical and Health Information
  - Rack
  - Position
  - ID
  - Bar Code
  - Patient ID
  - Collection Time
  - Test Date
  - Ordering Date
  - Operator
  - Ordering Department
  - Diagnosis
  - Ordered By
  - Comment

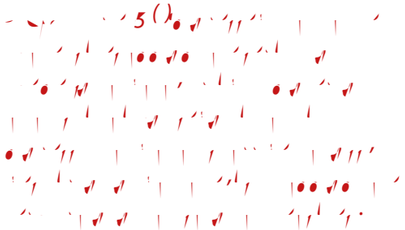
3. Storage Limitation



Mindray products support users to adhere to the GDPR principle of Storage Limitation. Our products enable a built-in function that can delete patient information stored in it when it is no longer necessary or after it is used. Our users can use this function to clear all sensitive personal data according to internal data retention policies or at the data subject's request. As role of processor, Mindray products will help controllers (e.g. hospitals) to facilitate them better managing data in compliance with GDPR.

For example, Mindray IVD products can keep a record of test results during a certain period. The maximum of samples stored in the system is 50,000. In addition, the results with the earliest date will be overridden when the capacity is exceeded. The user can delete used samples manually to free more disk space.

4. Integrity and Confidentiality



Mindray always highly values the security of the personal data. Mindray ensures that all personal data will be protected against unauthorised or unlawful processing and against accidental loss, destruction or damage. In Mindray, we take a layered approach to security – using both technology and managerial methods.

For example, Mindray MIS products have a Patient Data Management System to manage and protect patient data records. A patient data record consists of the following information:

- Patient basic information and exam data
- Image files
- Report

In order to better manage the records, the Patient Data Management System supports users to save, edit, delete and transfer patient data. Furthermore, the MIS products have Access Control which sets two different types of user accounts : Administrator and Operator.

- Administrator

  The system administrator can view all patient data, such as patient information, image and report, etc;

- Operator

  The operator can only view the exam information saved in the system and operated by himself or herself, such as patient information, image and report, etc. The operator cannot view the exam data operated by others.

Login to the system requires a correct password to identify your account type. This safety control is to prevent improper use for the system. Meanwhile, Mindray also notifies users that their password is sensitive and suggests to change it when logging into the system for the first time.

An exam record consists of all information and data of one exam. An exam record consists of the following information:

- Patient basic information and exam data
- Image files
- Report

NOTE:

1. DO NOT use the internal hard drive for long-term image storage. Daily backup is recommended. External storage media is recommended for image archive.
2. The system patient database space is limited, please back up or clear patient data in time.
3. Mindray is not responsible for lost data if you DO NOT follow suggested backup procedures.

5. Accountability

According to GDPR, Mindray implements not only internal and publicly-facing policies, records and notices, but also technical measures, and fundamental personnel and stra.5 (al)-1.sm r0.7en2to tn log(o)J .6 (m f)-1.2 (o)-2.3 2.7 (t o45 (c)4.6 r(g)-1.7 (n2)5 (A)12-6.9 (al)-pr -1.33D)-8-1.8 (o2-3.1 (3)J1 (

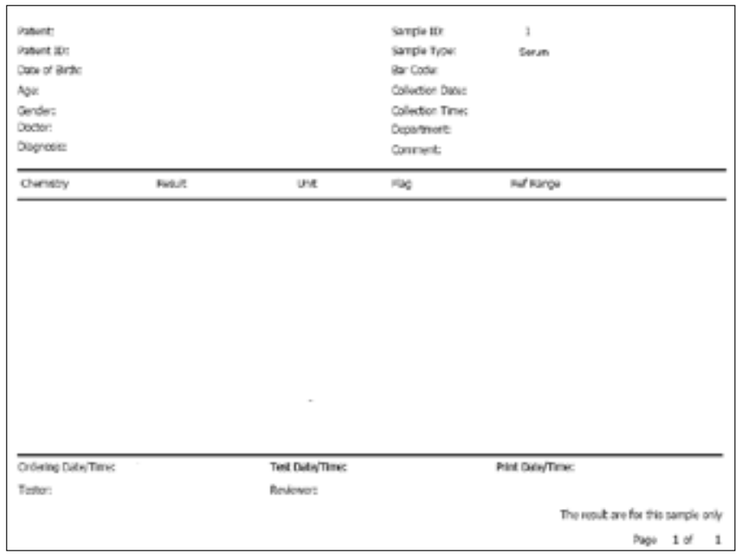
GDPR Rights of the Data Subject

The incoming GDPR will provide data subjects with enhanced rights over the use of personal data. Through these rights, data subjects can make a specific request and be assured that personal data is not being misused for purposes other than the legitimate purpose for which it was originally provided. Mindray always puts the user's needs in top priority while pursuing advanced technology. To help you better understand Mindray's efforts, we explain it specifically as following :

1. Right of access by the data subject

Mindray products can facilitate our users, namely the controllers, taking appropriate measures to provide information relating to processing of personal data in a concise, transparent, intelligible and easily accessible form. Mindray products are able to generate a standard electronic report automatically, which demonstrates what data will be collected and how to process it.

For example, Mindray IVD products can generate a report for patients that consists of three parts. The first part is patient information used for identification purposes. The second part is testing parameters and results. The third part is relevant information used for audit trail. There is a sample report as follows :



2. Right to rectification

According to GDPR, data subjects have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Hence, Mindray has designed the system function correspondingly to help the controller respond to the data subject's enquiry in a timely fashion and enable to make rectifications accordingly.

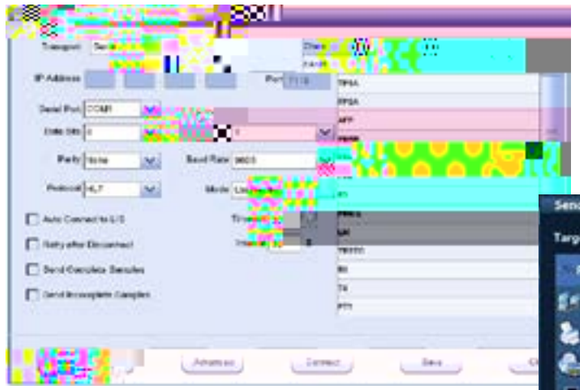
Mindray MIS products design iStation module which is a patient data management system. It is easy for users to manage and rectify patient data, including basic patient information, exam information, image files and reports.

When select a specific patient in the Patient List, you can perform the following functions from the drop-down menu.

3. Right to erasure

The Mindray IVD products can transfer or export testing results via Internet to Laboratory Information System (LIS). LIS is an external host computer connected with the IVD products through a fixed interface. The LIS is a set of standards widely adopted by medical industry so that patient's information can be transmitted without barriers.

The Mindray MIS products support the storage of patient data files either in an internal system (e.g. hard disk) or to external memory devices (e.g. USB devices, DVD-RW, CD-RW). To better manage saved patient data, MIS products design the Review control panel that integrates some essential functions and provides a user-friendly interface.



The page is intentionally left blank