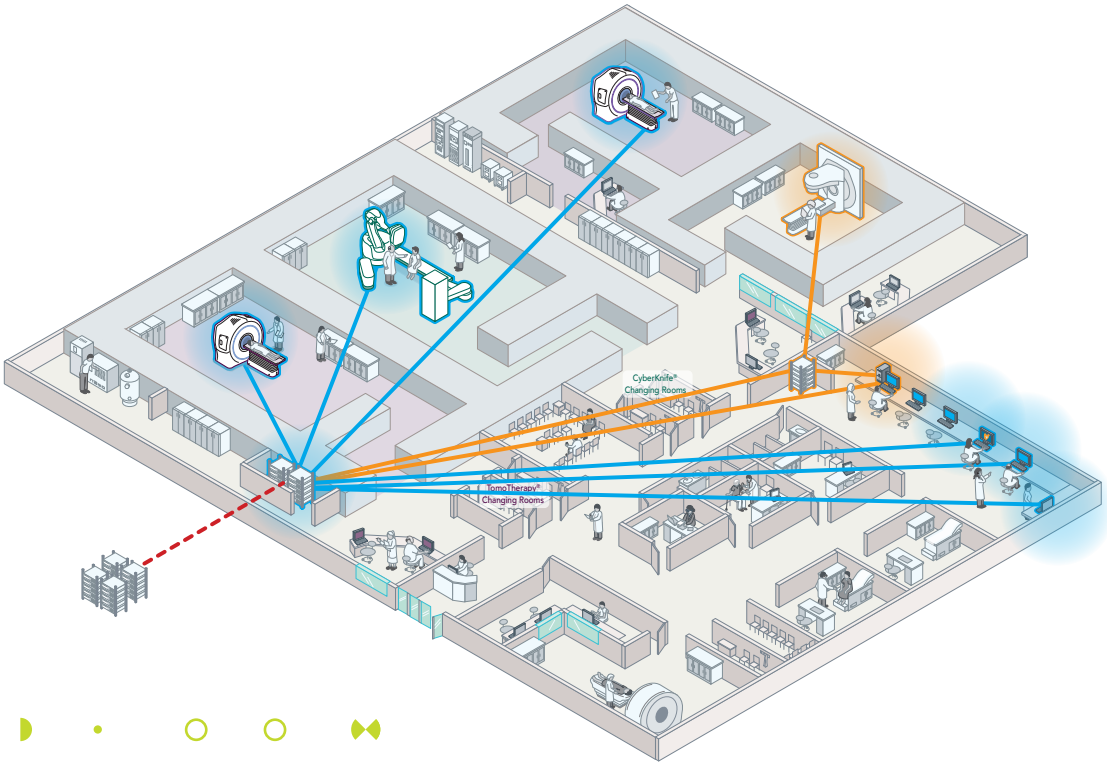
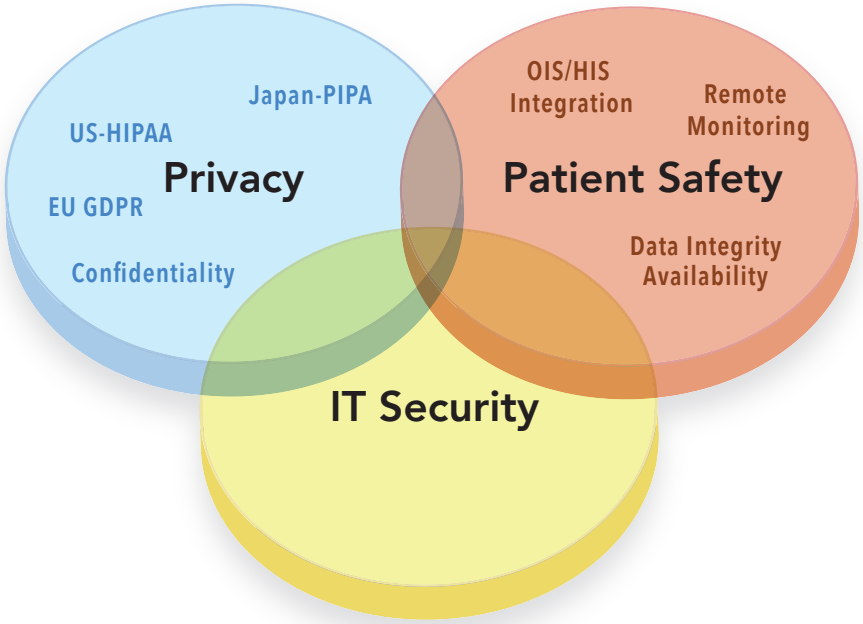
iDMS® INTEGRATED DATA MANAGEMENT SYSTEM WITH iLINK DATA FLOW

Accuray Incorporated





INTRODUCTION & BACKGROUND

As medical devices evolve to incorporate more software code, dedicated operating systems and networking devices, they are exposed to the same cyber-threats as conventional IT systems. For example, medical devices can be infected by malware or hacked, which can impact care delivery, potentially interfere with specified control, or lead to the breach of sensitive healthcare information. With threats to the security of devices increasing, governments have enacted legislation to criminalize many of these cyberattacks and protect identifiable health information.

AdvaMed Medical Device Cybersecurity Foundational Principles provide a template for addressing cybersecurity throughout the product lifecycle, including during the design, development, production, distribution, deployment, maintenance and disposal of the device and associated data.

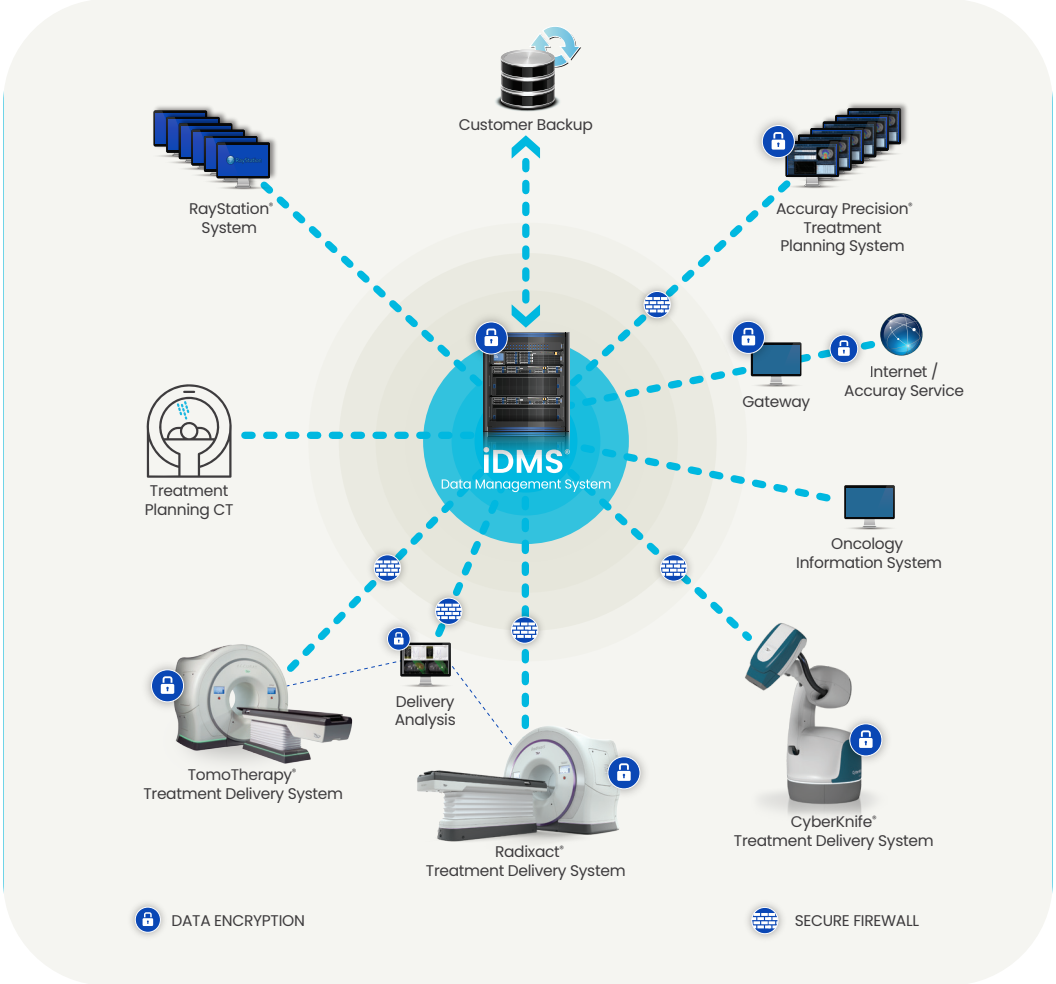
To address all inherent risks, manufacturers must appropriately employ a multi-modal strategy leveraging people, process and technology — both home-grown or outsourced to industry experts.

It is through this multi-modal approach that Accuray products can address strict standards for security while ensuring the expected standards in patient care and ease-of-use.

ACCURAY PRODUCT SECURITY: FOCUS ON iDMS®-ENABLED SYSTEMS

Accuray has centralized data-management of its treatment delivery systems and software within the iDMS® Integrated Data Management System. This is a single, secure data-server that allows customers to easily access and share patient treatment data across any Accuray radiation therapy platform. At the same time, this centralized architecture has a robust set of security features to prevent unauthorized access while enabling patient privacy and customer ease-of-use.

As a centralized repository, iDMS-enabled products are designed with the following security measures.



SECURITY

- All Windows-based machines include a white-listing security application that only allows pre-defined, signed applications to operate. This protects the system against viruses and operating system vulnerabilities that could permit the deployment of viruses or malware. White-listing security application does not require regular updates. It also ensures that only compatible versions of Accuray software are used.
- All computer systems associated with our devices can be placed behind the included firewall. Accuray Precision® workstations may also (by customer request) be placed outside the firewall on the customer's network.
- Accuray uses network segmentation for performance and security purposes within the treatment system, and between the customer's network and the product network primarily for security purposes.

AUTHENTICATION/AUTHORIZATION

- Accuray systems include site-defined users and passwords. This mechanism is complemented with role-based access including a tool to define permissions per role. Patient/System data can only be accessed after the appropriate authentication has occurred. Users can view actions taken within the system within the patient and system audit logs.
- **Passwords** are maintained in the iDMS® database in an encrypted format at rest and in-motion. When storing encrypted passwords in iDMS, the passwords are **hashed** to protect against an attack on the database (where by knowing one password would allow a hacker to compromise all passwords on the system).
- iDMS supports an **authentication** model that protects against repeated failed attempts to login to the system. Users that exceed the number of failed authentication attempts are temporarily disabled.

DATA INTEGRITY

- Accuray employs encryption technologies to protect sensitive data: iDMS and Accuray Precision® encrypt all data on the file system. While Radixact® encrypts all patient data and CyberKnife® anonymizes all data on disk.
- Data is protected on the iDMS server by use of hard drives configured in a RAID 6 array. This ensures that up to 2 hard drives per array can fail prior to losing any data. Furthermore, Accuray remote monitoring can proactively warn of disk failures.
- iDMS provides file-level data integrity checking, preventing a corrupted or infected data file from being used by the system.
- Accuray provides security updates to critical systems, such as the treatment delivery system, with major software upgrades.

PRIVACY: PERSONAL DATA PROTECTION

For iDMS-enabled systems, Accuray has applied privacy-by-design principles that enable deidentification of patients' health information. Additionally, the control to transfer patient data to Accuray is at the discretion of the hospital. In the event a user intends on transferring data to Accuray, the site must manually place patient data into predefined system directories that allow Accuray personnel to access the needed information. Finally, encryption features for data at rest have been included in iDMS-enabled systems:

- Data on treatment systems is encrypted and can be de-identified in such a fashion as to remove any direct identifiers.
- When backing up patient data to a customer-provided network location, the data is automatically encrypted.
- Accuray protects PHI during service events of iDMS-enabled systems: 1) patient data if required, is de-identified prior to upload 2) log file data does not contain patient direct identifiers.

Remote Connectivity through the IoT (Internet of Things)

Accuray systems share information in real time with Accuray support teams. These include crucial system- performance data that help prevent system failures. As well as 1-on-1 support sessions with Accuray clinical and technical support.

Remote Connectivity is managed through PTC Machine Cloud Service, a powerful, industry-leading data management technology. This secure, encrypted connection includes explicit authorization and authentication controls to ensure secure access to all information during service sessions. PTC has attained ISO 27001:2013 certification and SOC 2 Type II, supporting their focus on delivering the highest levels of security, performance and availability of the PTC Machine Cloud Service.

iLink is an Accuray-built product that interfaces with PTC components to establish a service connection with Accuray systems to enable remote machine diagnostics. For pre-iDMS products, Accuray makes use of Remote Service Node (RSN) to connect to PTC ThingWorx Cloud.

PTC Thingworx
PTC ThingWorx provides Accuray single tenant SaaS platform and client applications to collect machine data, alarms and logs and access the system remotely for service maintenance. PTC ThingWorx provides all the capabilities for device management.

Security Monitoring
PTC Thingworx uses antivirus, firewall and intrusion detection system for continuous security/compliance monitoring and log analysis, coupled with 24x7 monitoring services from PTC security operations center. Leveraging a wide variety of monitoring services, PTC Thingworx provides a high level of service performance, awareness, and availability. These monitoring services are implemented to detect unusual, unauthorized, or unanticipated activities and conditions at inbound/ outbound communication points, on systems/ servers, and within the applications operating within the hosting environments.

Data Security
Data is encrypted in transit using HTTPS/TLS (Transport Layer Security). TLS 1.2 with AES 128-bit key encryption is default for communication with customers. Default cipher for use in communication between the platform and client application is TLS_RSA_WITH_AES_128_CBC_SHA.

Security Assessment
PTC Thingworx evaluates the infrastructure, data, software, and procedures as part of its ongoing risk assessment process and conducts vulnerability scans every 2 – 3 months, penetration test at major release, and annual security assessment.

Patch and Update
Accuray monitors security vulnerabilities of the platform and applications and implements security patch via product development process and post-market surveillance process if patch is required. Application software patches and updates are applied to PTC Thingworx cloud platform.

iLink/RSN includes automatic collection of:

- System alarm events (i.e. hard drive failure, server temperature, etc.)
- Machine procedure data files including:
  - → System sensor measurements (i.e. gun voltage, coolant flow, injector current, etc.)
  - → System workflow time measurements (i.e. procedure begin, warm-up begin, etc.)
  - → Error messages (i.e., procedure interrupted)
- System log files containing:
  - → Software diagnostic messages
  - → System error information
- Additionally, this secure connection can be used to:
  - → Manually upload data files to Accuray
  - → Remotely access systems using a site approved remote desktop sharing sessions

Identity & Access Management
For device–level authentication and authorization, PTC ThingWorx makes use of server certificate–based authentication and device ID to address issues of authentication, impersonation/ tampering. By default, ThingWorx's out-of-the-box edge agent (WebSockets Edge Microserver) always attempts to connect to ThingWorx platform using TLS. TLS allows client/server applications to communicate in a secure way that is designed to prevent eavesdropping, tampering, or message forgery.

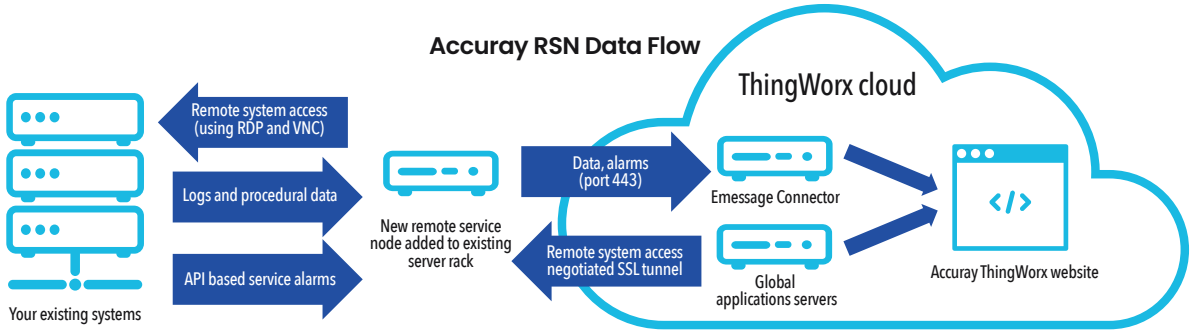
Platform Backup & Disaster Recovery
All PTC Thingworx backups run automatically and notify the team off success or failure. If a failure occurs, the backups are reviewed and run manually. A random set of backups are tested on an annual basis. Backups are stored at the primary, local hosting facility for a period of 30 days and stored for 90 days in a replicated off-site, DR facility daily. Backups at the Disaster Recovery facility are kept for a period of one year. RPO (Recovery Point Objective) is 24 hours, RTO (Recovery Time Objective) is 5 business days. All backup data are encrypted.

Certifications and Audits
PTC Thingworx is ISO 27001: 2013 certified and maintains SSAE16 SOC 2 Type II Security & Availability Trust Principles. By being audited by third-parties, PTC Thingworx maintains a rigorous Security and Compliance program in alignment with the ISO framework, the SSAE16 SOC 2 Type II Security & Availability Trust Principles.

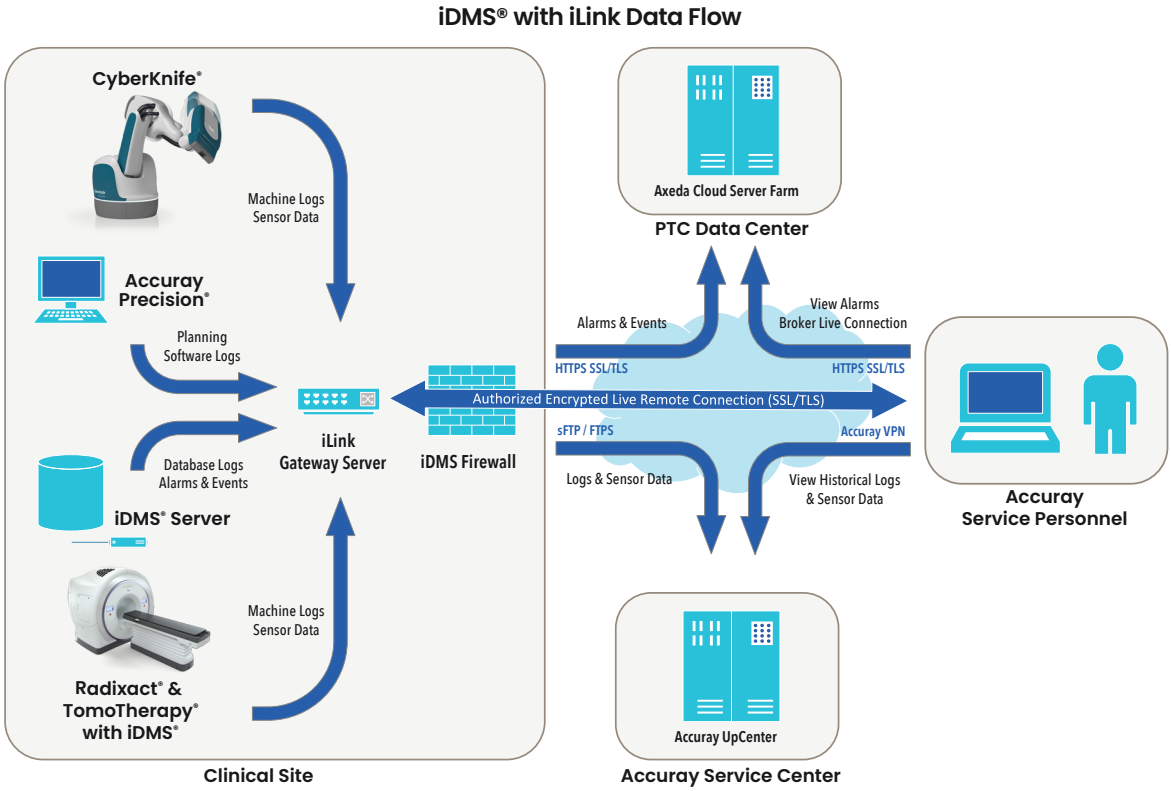
Additionally, PTC Thingworx has implemented various risk reduction controls, including administrative and physical assets to manage access to computing systems and physical facilities.

Data is transmitted through encrypted iLink/RSN and kept secure using:

1) Transport layer security (TLS) at the communications level.
2) Advanced encryption standard (AES) 128 algorithm
3) The RSA 2048 algorithm for key data exchanges.



A global infrastructure connects Accuray sites to the ThingWorx Cloud via gateway edge device clients, Emessage Connector hosts, a Global Access Server Network and Azure hosted ThingWorx Cloud instances.



GoToAssist

- For real-time technical support and remote access, Accuray has partnered with LOGMEIN.
- LOGMEIN's GoToAssist® is an on-demand application, enabling remote service sessions with Accuray support teams: Service Engineers, Clinical Applications and Physics. While their GoToMyPC® Corporate product is an optional remote desktop application that allows users to access Accuray treatment planning systems and data remotely within an organization's secure network.
- LOGMEIN has set an industry standard with adoption of the ISO 27001 security framework, development of tools with embedded security controls and processes that are focused on cybersecurity. Both applications employ SSL technology and 128-bit AES encryption.

CUSTOMER RESPONSIBILITIES

- Customer is responsible for putting in place appropriate internal controls to manage system passwords and user access. This should include password strength requirements and controls for disabling access to exiting employees.

- Accuray software products should be used only on computers and networks that are properly secured in accordance with Accuray product documentation, service agreements, and instructions for use.

- Accuray systems and accessories do not permit third-party software installation by the customer (e.g., anti-virus scanners, office productivity tools, system patches, on-platform firewalls, etc.) unless documented by Accuray as an operating specification or prior written consent is attained. Unauthorized modifications to Accuray products could void warranty and alter the regulatory status of the device. Any resulting service required from unauthorized modification is not covered under our service agreements. Such unauthorized modifications can affect the performance or safety of your device in unpredictable ways. Accuray is not responsible for equipment that has been subject to unauthorized modification.

- Accuray recommends users backup data on the hospital network so that in the case of a data loss event, a solid backup for restoration by Accuray Service personnel is available

- Accuray does not encrypt network data transmissions. It is the customer's responsibility to protect network and data transmission infrastructure from internal and external threats. This includes maintaining data security requirements and point-to-point encryption among the Accuray System firewall and the following potential data destinations or access points: The dedicated Virtual Local Area Network (VLAN), Accuray Precision® System workstations, Wide Area Network (WAN) Connected Treatment System, the redundant iDMS System installed on a facility Local Area Network (LAN) or WAN.

Conclusion

Responsible medical device companies assess, mitigate, and constantly monitor the ever-present cybersecurity threats to critical assets. Medical device manufacturers, healthcare service providers, patients, and physicians are collectively responsible for collaborating to create a resilient, secure approach that embraces technological innovation while mitigating its associated risks. With increased information sharing, constant monitoring, and an informed understanding of the threats they face, medical device manufacturers can assess potential vulnerabilities and identify risk mitigation strategies that will ultimately strengthen security. Accuray continues to examine and evolve existing products to best accommodate the requirements of Accuray's security-minded customers while enabling a 'Patient-First' clinical practice.

Additional Information

Considering the increased focus on medical device security and compliance with the HIPAA Security Rule in the US, the Healthcare Information and Management Systems Society (HIMSS) created a standard “Manufacturer Disclosure Statement for Medical Device Security” (MDS2). The MDS2 is intended to supply healthcare providers with important information that can assist them in assessing and managing the vulnerabilities and risks associated with the electronic Protected Health Information (ePHI) that is created, transmitted, or maintained by medical devices. Accuray MDS2 forms are available to customers upon request.

LOGMEIN Resources

HIPAA Compliance Guide
https://www.gotomypc.com/downloads/pdf/m/GoToMyPC_Corporate_HIPAA_Compliance_Guide.pdf

Corporate Security White Paper
https://www.gotomypc.com/downloads/pdf/m/GoToMyPC_Corporate_Security_White_Paper.pdf

GoToAssist: "Remote Support Security for the Modern Enterprise"
https://assets.cdngetgo.com/18/f0/2bf0fd0b4c9b8cfff91eb6addf38/gotoassist-corporate-security-whitepaper.pdf

Platform specific IT guides for Accuray CyberKnife®, TomoTherapy® and Radixact® Systems can be requested through support@accuray.com or by calling 1.877.668.8667

ACCURAY

UNITED STATES

Accuray Corporate Headquarters
1310 Chesapeake Terrace
Sunnyvale, CA 94089
USA
Tel: +1.408.716.4600
Toll Free: 1.888.522.3740
Fax: +1.408.716.4601
Email: sales@accuray.com

Accuray Incorporated
1240 Deming Way
Madison, WI 53717
USA
Tel: +1.608.824.2800
Fax: +1.608.824.2996

ASIA

Accuray Japan K.K.
Shin Otemachi Building 7F
2-2-1 Otemachi, Chiyoda-ku
Tokyo 100-0004
Japan
Tel: +81.3.6265.1526
Fax: +81.3.3272.6166

Accuray Asia Ltd.
16/F, Tower 5, The Gateway
Harbour City
15 Canton Road, T.S.T
Hong Kong
Tel: +852.2247.8688
Fax: : +852.2175.5799

Accuray Accelerator Technology (Chengdu) Co., Ltd.
No. 8, Kexin Road
Hi-Tech Zone (West Area)
Chengdu
611731 Sichuan
China

EUROPE

Accuray International Sarl
Route de la Longeraie 9
CH – 1110 Morges
Switzerland
Tel: +41.21.545.9500
Fax: +41.21.545.9501

Important Safety Information:

Most side effects of radiotherapy, including radiotherapy delivered with Accuray systems, are mild and temporary, often involving fatigue, nausea, and skin irritation. Side effects can be severe, however, leading to pain, alterations in normal body functions (for example, urinary or salivary function), deterioration of quality of life, permanent injury, and even death. Side effects can occur during or shortly after radiation treatment or in the months and years following radiation. The nature and severity of side effects depend on many factors, including the size and location of the treated tumor, the treatment technique (for example, the radiation dose), and the patient's general medical condition, to name a few. For more details about the side effects of your radiation therapy, and to see if treatment with an Accuray product is right for you, ask your doctor. Accuray Incorporated as a medical device manufacturer cannot and does not recommend specific treatment approaches. Individual results may vary.