PHILIPS

Enterprise Imaging

White paper

General Data Protection Regulation (GDPR) compliance

The General Data Protection Regulation (GDPR) gives people in the European Union (EU) greater control over how organizations use their data, and imposes heavy penalties for organizations that fail to comply with the rules and for those whose data has been breached.

The Philips approach to privacy

At Philips, we believe that putting trust, transparency and control at the heart of our customer and consumer experience is key to being a successful health technology company. We have been closely monitoring the progress of GDPR and partner with, as well as employ, numerous legal, process and privacy experts who help us to navigate these regulatory challenges and to deliver on our commitments.

In 2009, Philips implemented the Binding Corporate Rules and is continuously working with the current European Data Protection Directive, as well as national legal regimes governing the collection and use of personal data, both inside and outside the EU. Consequently, Philips has had processes and mechanisms in place that facilitate individuals in the EU to exercise their rights in a similar manner to that prescribed by the GDPR. We have worked diligently to update our processes where necessary in advance of the GDPR 2018 implementation date.

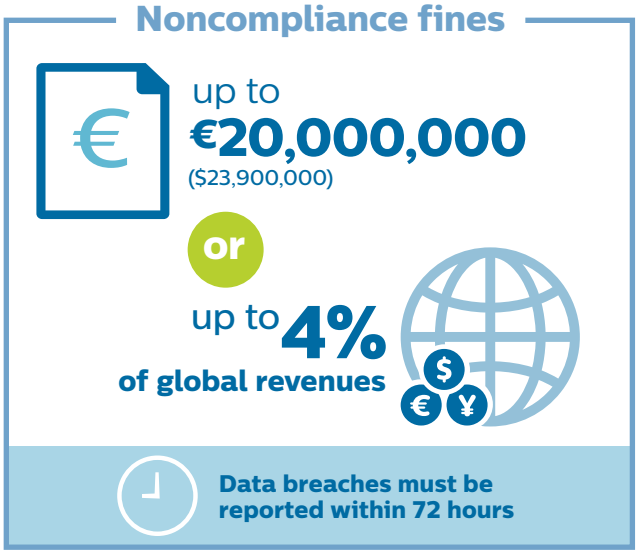
Data controllers vs data processors

Both data controllers and data processors are required to abide by the GDPR. A data controller is responsible for how and why personal data are processed. A data processor actually processes the data. A controller could be any organization, from a profit-seeking company to a charity or government. A processor could be an IT firm doing the actual data processing. Philips Radiology Informatics (RI) is a data processor for our customers.

It is the controller's responsibility to ensure their processor abides by the data protection law and processors must themselves abide by rules to maintain records of their processing activities. Even if controllers and processors are based outside the EU, the GDPR applies to them as long as they're dealing with data belonging to EU residents.

The costs of noncompliance

Under the GDPR, costs of noncompliance include administrative fines of up to €20,000,000 or up to 4% of an entity's global revenues, whichever is higher. And of course, the cost to reputation in the case of a security breach is nearly incalculable.



A closer look at the GDPR

Here are steps Philips has taken to comply with the GDPR.

Organization

The GDPR establishes accountability for privacy, specific organizational roles and responsibilities, documentation of privacy policies and procedures, and registration activities with local regulatory authorities. Philips has updated relevant policies to comply with GDPR. In preparation for GDPR, roles and responsibilities have been reviewed and socialized to help define contact points for employees. Philips RI has a dedicated care organization with several levels of support (L1/L2) with segmentation of network and access to comply with minimal exposure of personal data. There are specific obligations defined for each role/organization and continuous internal training to stay up to date on procedures and regulations, per role and responsibilities. In addition, business innovation units have their own general manager and accountability.

Notice

The GDPR requires notification of the organization's privacy practices, including how personal data about data subjects are protected and the purpose for which personal data are collected, used, retained and disclosed. Philips has updated policies and included appropriate considerations on GDPR.

Choice and consent

Requirements of the GDPR provide data subjects with a choice about how their personal data may be used, and to obtain their consent for the collection, use and disclosure for primary or secondary purposes. Philips Privacy Office has reviewed contract templates that will enable Philips Radiology Informatics (RI) to maintain and commence relationships with business partners in a compliant manner with respect to GDPR.

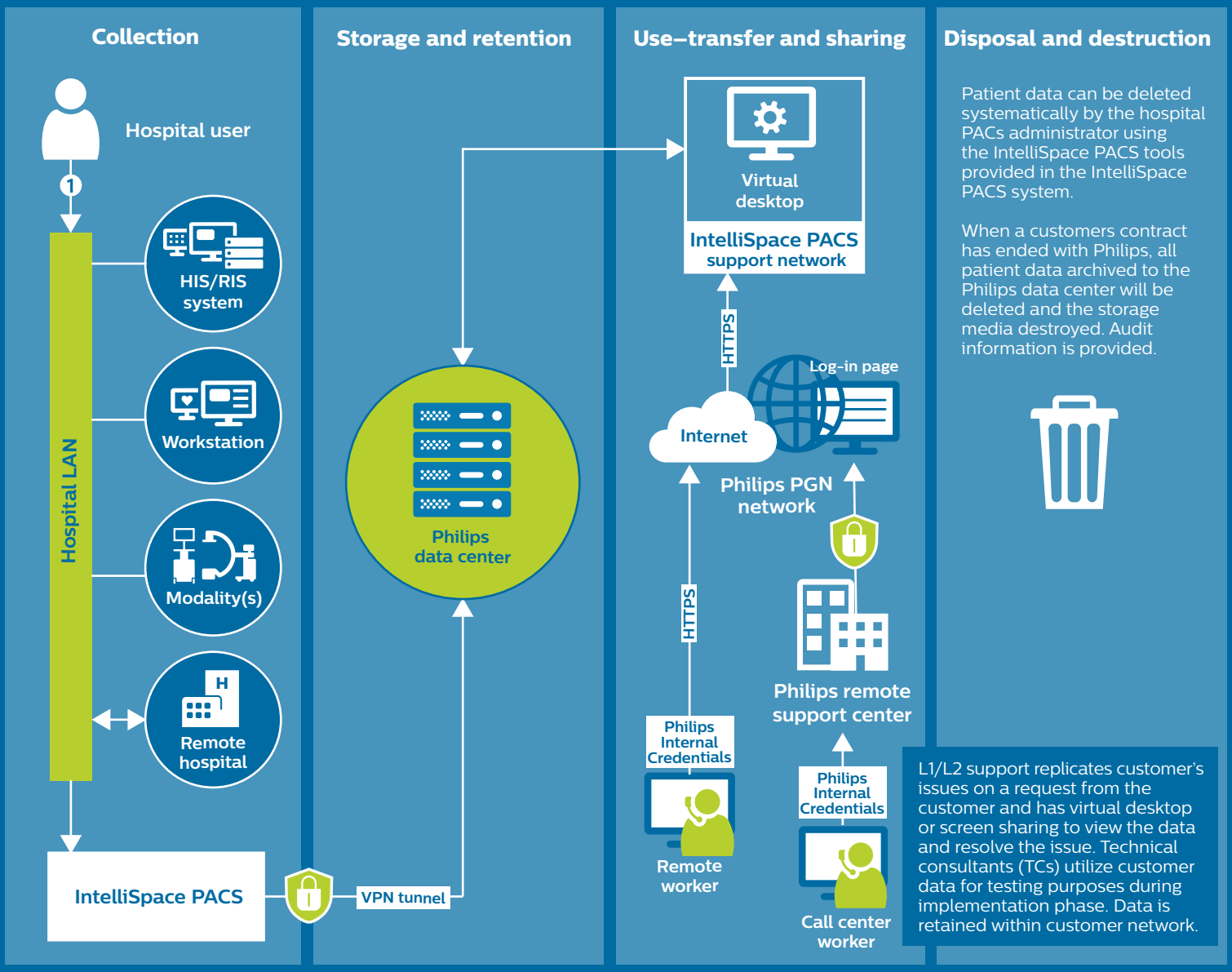
Access, correction, amendment, deletion

This GDPR requirement permits data subjects access to personal data that the organization may have about them. Philips has a formal process to support a deletion request when a contract for services has ended.

Security for privacy

The GDPR includes requirements to provide administrative, technical and/or physical security controls to prevent unauthorized or accidental loss, corruption or disclosure of personal data. Philips has streamlined the quality management system (QMS) process to approve review of updated security-related policies and procedures to support GDPR requirements. Philips uses a de-identification process so that this data is kept private and separately. Data are encrypted and secured via the IPSEC VPN tunnel. Customer site remote access information is collected 24/7/365, with audit data available upon request.

IntelliSpace PACS data flow security and patient privacy



Data key
1. Patient health data

Transfer and disclosure

Representative requirements of the GDPR concern the disclosure of personal data to third parties and the transfer of personal data to other countries. Philips has Binding Corporate Rules to support international transfers of data that have been updated to demonstrate GDPR compliance. Additionally, third-party contracts are being updated to reflect that third parties must not process personal data except on instructions from the controller as relayed by Philips. Philips managed service provides 24/7 global service support, and is proactively and remotely monitored. Contracts offer fixing and patching programs to maximize performance.

Information management data lifecycle

The GDPR has representative requirements that include the collection, use, storage and destruction of personal data. Philips has a formal process to support a deletion request when a contract for services has ended. Philips RI has formal quality and regulatory processes to support a deletion request. Hospital administrators have the ability to delete patient data. This deletion occurs across the migration chain to the Philips data center.

Data quality

The GDPR is concerned with the quality of information about data subjects and how personal data are processed. This may include the organization's efforts such that any personal data collected are accurate, complete and up to date. Patient data are authentic and intact due to encryption at rest and in transit. Our hardened computer environment means data stay within defined network and storage boundaries.

Monitoring and enforcement

The GDPR requires periodic monitoring such that the organization complies with its privacy policies and procedures, and the extent to which data subjects have recourse to bring forward inquiries and/or complaints.

Breach notification

The GDPR requires notification of relevant parties in the event of accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data where this may lead to risk for the data subjects/individuals affected. Philips maintains product security and privacy-specific incident response documentation and has a comprehensive cyber incident response plan that outlines the interactions between business groups. For Philips RI this includes internal qualification of the breach, internal notification to field employees of the information that should be communicated to customers, a customer letter sent by the Philips RI service rep (customer success manager), and a proposal to fix the breach with a remote patching program or upgrade. A disaster recovery plan is also offered with our managed service model.

Outstanding care delivery starts with the right partnership

Philips is committed to offering a managed service that addresses the challenges of today's healthcare organizations in protecting investments, securing patient privacy and safety, and increasing efficiency.

philips.com

Printed in The Netherlands.
4522 991 37321 * JUL 2018