Vue Cloud Information Security Policy for Europe

Version: v1.6

Table of content

1 Introduction

In the document, ***Vue Cloud Services*** refers to ***Carestream Vue for Cloud-based Services***.

This document is the **Information Security Policy** (ISP) for the Vue Cloud Services provided by Carestream in Europe. This ISP states the commitment of the top management to the strategic importance of the information security management system for Carestream business. The policy guides and directs all information security activities in the organization.

Information should always be protected, whatever its form and however it is shared, communicated or stored. Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or by using electronic means, shown on films, or spoken in conversation.

Information security is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities. It also covers the requirements from legal obligations and contractual agreements to protect information.

This ISP constitutes the foundation document for the process of information security as implemented by Carestream HCIS Europe within its Vue Cloud Services and covering all information systems implied in these services. It defines the framework for this process, in accordance with the agreement of the management of Carestream HCIS Europe. Therefore, it transcribes the strong support of the management of Carestream HCIS Europe in setting up and maintaining this approach to information security.

Note - This ISP is the information security policy as required by ISO27001:2013 (Section 5.2).

2 Scope

This policy supports the provision of Vue Cloud Services by Carestream HCIS Europe. It applies to all entities, divisions, personnel of Carestream HCIS Europe implied in Vue Cloud Services: Services Delivery, Services Operations, Services Support, Solution Architect and Business Development. It also covers support activities (management of HR, management of suppliers, customer relationships…).

The suppliers, whether they are in other entities, regional areas of Carestream or outside Carestream, are not directly in the scope of this policy, but the management of the relationship with these suppliers is in the scope, in order that these suppliers provide products and services compliant with information security requirements from Carestream HCIS Europe.

3 Objectives

The main information security objectives of Carestream HCIS Europe regarding Vue Cloud Services are:

- Information security risks of Vue Cloud Services are understood and treated to be acceptable to the Carestream HCIS Europe;
- The confidentiality of patient data, customer information, product development and marketing plans is protected;
- The integrity of patient data and accounting records is preserved;
- External and internal networks meet specified availability standards;
- The conformity with regulation of each country, regarding the protection of personal data and healthcare data is ensured.

4 Principles

The main principles applied to the information security process are:

- Carestream HCIS Europe encourages initiative and risk taking as long as the risks are understood, monitored and treated appropriately;
- All staff will be made aware and accountable for information security as relevant to their job role;
- Provision will be made for funding information security controls in operational and project management processes;
- Possibilities for fraud associated with abuse of information systems will be taken into account in the overall management of information systems;
- Information security status reports will be available;
- Information security risks will be monitored and action taken when changes result in risks that are not in line with the organization's policies and procedures;
- Situations that could place the organization in breach of laws and statutory regulations will not be tolerated, especially regarding the protection of healthcare data and personal data (privacy);
- All data on storage media replaced because of failure or upgrade, or moved away, must be destroyed to prevent any unwanted data recovery, therefore Carestream teams and external partners must commit on data erasure in such case.

5 ResponsIbilities

The global responsibilities regarding information security are:

- The executive management team of Carestream HCIS Europe is responsible for ensuring that information security is adequately addressed throughout the organization;
- Each manager is responsible for ensuring that the people who work under their control protect information in accordance with the organizations standards;
- The chief security officer advises the executive management team, provides support for the organization's staff, and ensure that information security status reports are available;
- Every staff member has information security responsibilities as part of their job role.

CARESTREAM is a trademark of Carestream Health, Inc.

© Carestream Health, Inc. 2016
150 Verona Street
Rochester, NY 14608
United States