BEACON HEALTHCARE SYSTEMS	Information Technology Department **Policy Document**

Data Protection & Privacy Policy

Version 2.1
11th May 2024

History Log		
Version	**Date**	**Author**
Version 1.0	Jun 2020	Beacon HCS
Version 2.1	May 2024	Beacon HCS

Contents

1. Purpose

The purpose of this policy is to ensure protection of Beacon HCS's sensitive data / information, including Card Data, PII and PHI, at storage and in transit with industry accepted encryption standard.

2. Scope

This policy document addresses Beacon HCS data encryption and key management requirements for Sensitive Data in transit and in storage.

3. Policy

3.1 Render sensitive data, at minimum, unreadable anywhere it is stored (including data on portable digital media, backup media, in logs, and data received from or stored by wireless networks) by using any of the following approaches:
a) Strong one-way hash functions (hashed indexes)
b) Truncation
c) Index tokens and pads (pads must be securely stored)
d) Strong cryptography with associated key management processes and procedures

3.2 Encryption of sensitive data shall be carried out using Symmetric Key Encryption: AES 256 bits, or 3DES with associated Key management procedures Asymmetric Key Encryption: RSA 2048 Bits, Deffie Hellman 2048 Bits, El Gamal 2048 Bits

3.3 Sensitive data on removable media shall be encrypted wherever stored.

3.4 If Disk encryption is used for encrypting the data then logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts.

3.5 No sensitive data shall be sent via end-user messaging technologies for example e-mail, instant messaging, and chat, unless with approval from Information Security and with appropriate

security controls in place. If there is a business requirement where data is to be sent over email then it must be encrypted with strong encryption algorithm to ensure secure communication.

3.6 Any sensitive data transmission over public networks (e.g. Internet, wireless, Cellular technology – GSM & CDMA, GPRS, Satellite communication) must be encrypted using strong cryptography and security protocol (e.g. IPSEC VPN, SSL, SSH, etc.) to safeguard data during transmission. Also, the following needs to be considered in such cases:

- Only trusted keys and certificates are accepted.
- The protocol in use only supports secure versions or configurations e.g. SSL v3.
- The encryption strength is appropriate for the encryption methodology in use e.g. AES256, RSA 2048, 3DES.

3.7 Encryption Keys shall be stored in a location separate from the encrypted data.

3.8 Store keys securely in the fewest possible locations and forms.

3.9 Cryptographic keys used to encrypt/decrypt sensitive data must only always exist in one (or more) of the following forms. Please document the procedures for each of the bullet points listed here as per actual implementation of encryption mechanism in environment).

- Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key.
- Within a secure cryptographic device (such as a host security module (HSM) or PTS-approved point-of-interaction device).
- As key components or key shares, in accordance with an industry-accepted method.

3.10 Encryption keys used for encryption of sensitive data shall be protected against both disclosure and misuse by:

- Restricting access to keys to the fewest number of custodians necessary
- Secure storage of keys in the fewest possible locations and forms

3.11 Key management processes and procedures for keys used for encryption of sensitive data shall be documented and implemented for (must document the procedures for key generation, storage, distribution and each of the bullet point listed here as per actual implementation of encryption mechanism in environment):

- Generation of strong keys
- Secure key distribution
- Secure key storage

- Periodic key changes
  - as per crypto period of encryption algorithm
  - In case of suspicion of key compromise or when person with knowledge of key leaving the job
- Destruction of old keys.
- Split knowledge and establishment of dual control of keys (so that it requires two or three people, each knowing only their part of the key, to reconstruct the whole key
- Prevention of unauthorized substitution of keys
- Replacement of known or suspected compromised keys
- Revocation of old or invalid keys (For RSA Keys only)

3.12 Encryption keys shall be changed or retired:

- as per defined crypto period of encryption algorithm
- In case of suspicion of key compromise or when person with knowledge of key leaving the job
- When the integrity of the key has been weakened.

3.13 Any keys retained after retiring or replacing are not used for encryption operations.

3.14 If manual clear-text cryptographic key-management operations are used, then use of split knowledge and dual control shall be followed to ensure that two people are required to perform any key-management operations and no one person has access to the authentication materials of another.

3.15 Requirement for key custodians to sign a form stating that they understand and accept their key-custodian responsibilities.

3.16 The organization has formally appointed a qualified data protection officer, reporting to senior management, and who is directly and fully responsible for the privacy of sensitive information.

3.17 When required, consent is obtained before any PII (e.g., about a client/customer) is emailed, faxed, or communicated by telephone conversation, or otherwise disclosed to parties external to the organization.

3.18 The confidentiality and integrity of sensitive information at rest is protected using an encryption method appropriate to the medium where it is stored; where the organization chooses not to encrypt sensitive information, a documented rationale for not doing so is maintained or alternative compensating controls are used if the method is approved and reviewed annually by the CISO.

3.19 Sensitive information is retained only for as long as required by regulatory, legal, or organizational requirements.

3.20 Organization has implemented technical means to ensure sensitive information is stored in organization-specified locations.

3.21 Following the death of any individual and if Beacon HCS must retain identifiable data for such individuals, it must be safeguarded protected for 50 years from the date of death.

3.22 Copies of any notices issued by Beacon HCS must be maintained for 6 years. If required, acknowledgment of receipt of such notices or any efforts to acquire any acknowledgment shall also be documented.

3.23 Any restrictions towards safeguarding of organizational records must be recorded in writing. Such records must be treated as organization and these or digital copies of these records must be maintained for 6 years.

3.24 The organization must record and retain as organizational record, for 6 years, a) Covered data that is subject to access by individuals and b) Designation of personnel or office that receives and processes applications of individuals who wish to access such data.

3.25 If any organizational record is disclosed, Beacon HCS must document and retain, for 6 years, such events as organizational records. This documentation must include, all details provided to the individual, all details requested from the individual to provide the records and designation of personnel or offices who receive and process such applications.

3.26 The organization will implement security and privacy protections of the transfer of organizational records, whole or in part, to a state, federal agency, or any other regulatory bodies.

3.27 Customers and the public shall be able to access all information regarding Beacon HCS's privacy controls and activities. Similarly, the public shall have the ability to communicate with the senior most privacy officer at Beacon HCS.

3.28 All policy, procedures, and other sensitive documents, including PHI disclosures shall be maintained for 6 years. All records of disclosures to carry out treatment, payment, and healthcare operations, that are electronic in nature, shall be retained for 3 years.

3.29 Security measures including, but not limited to, encryption, access control, electronic signatures, physical controls, and back-up processes shall be implemented to safeguard important documents like customer and vendor contracts, personnel records, financial information from loss or fraud.

3.30 Beacon HCS shall publish guidelines for all documents, records, and data, with regards to ownership, data and security classification, data handling, retention period, storage location and disposal process.

3.31 Security classification and all its principles must be reviewed and approved by the senior-most security and privacy officer within the company.

3.32 Beacon HCS must create a data retention program and it must cover a) a process of disposal of data once the retention requirements across legal, regulatory, and business factors are complete, b) extends the scope of the process to all storage areas for covered information. The program must also establish a process to distinguish and delete any covered information that has met the data retention requirements; this activity must be performed every 90 days by using both automated tools and manual techniques.

3.33 The data protection and privacy procedures shall include, a) schedule for retention of different types of essential records with the time-period for which they must be retained, b) a directory for sources of critical information. If cryptography is used, all cryptographic keys must be stored securely and must be made available only when required. Any information related to such keys and the encrypted, which will be required for decryption, must also be retained for the same time as the key and the data itself.

3.34 All covered information must be stored only for the minimum required time, factoring in the legal, regulatory, and business requirements. Also, the storage locations must be minimized as much as possible for all such information.

3.35 Beacon HCS must document and publish all locations where covered information may be stored.

3.36 The MINIMUM account information that must be rendered unreadable is the PAN.

3.37 Beacon Employees are not allowed to travel to High Risk locations with Beacon Devices.

The SVP of Engineering, Manish Nautiyal, is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the review requirements stated above.

A current version of this document is available to all members of staff.

This policy was approved by the SVP of Engineering and is issued on a version-controlled basis.

Date: 11th May 2024