Vitalerter 維特爾公司 有關安全性的技術說明

傳感器安全

該傳感器採用標準醫療級 Wi-Fi 模塊，該模塊根據 HIPAA NIST 特別出版物 800-52 規範要求，採用最高安全標準的加密。

加密

從傳感器到雲端的所有流量均根據 HIPAA NIST 特別出版物 800-52 規範要求進行加密和保護。

雲安全標準

Vitalerter 在 Microsoft Azure 雲中使用安全帳戶。 該帳戶符合 GDPR (歐盟一般資料保護規範) 和 HIPAA 安全規則，該規則制定了管理、技術和物理保護標準，以保護電子 PHI 免遭未經授權的訪問、使用和披露。

冗餘和備份

所有數據都存儲在 Azure 大數據存儲 blob 和 Azure SQL 服務中，每隔幾個小時備份一次，並且隨時可以恢復。 Azure 存儲在不同的故障域上存儲多個數據副本，並且默認情況下會將數據複製到備份數據中心 (如果需要，可以關閉異地複制功能)。

存儲加密

所有存檔數據都被加密。 所有數據均按照 45 CFR § 164.514(b) 進行加密，並將識別/加密密鑰單獨存儲在 BAA 範圍內的 Azure 服務中。

授權

所有服務和數據只能由授權人員使用獨特的、經過審核的訪問控制來訪問。 該系統使用符合 HIPAA 的雲活動目錄系統來管理訪問控制，因此只有具有相關權限的員工才能訪問 PHI 數據，僅限於其在組織中的權限。

數據匿名化

Vitalerter 維特爾公司 僅存儲匿名數據，因此系統開發人員無法識別患者身份。

在一些長照機構療養院，開發人員可能會意識到一般的非識別性患者詳細信息，特別是：年齡、性別和行動能力水平，但不會存儲進一步的識別詳細信息。 Vitalerter 維特爾公司 使用這些數據進行研究和改進系統，但為此我們僅使用數據的匿名和聚合視圖。 理想情況下，長照機構療養院應提前告知患者任何研究使用其個人數據的情況，但由於長照機構療養院正在共享匿名數據，因此他們沒有義務獲得患者的同意。 在一些療養院，我們要求從患者的醫療記錄中獲取更多信息。 重要的一點是，只要我們無法將數據集與可識別的個人關聯起來，我們就不需要徵得患者的同意。 如果我們在任何時候出於研究目的需要了解患者的身份，我們應該獲得患者的同意才能使用這些數據，但目前系統不存儲任何此類數據。

處理

當不再需要時，所有數據將被永久丟棄。 所有 SQL Server 數據將在 30 天后處理。 所有大數據均加密存儲並在 2 年後處置。

(英文正本如後續頁)

Tech-note about Security

VITALERTER
A vital leap to quality patient care

SENSOR SECURITY

The sensor is using standard medical grade Wi-Fi module that use encryption in the highest security standards according to the HIPAA NIST Special Publications 800-52 requirement.

ENCRYPTION

All traffic from the sensor to the cloud is encrypted and secured according to the HIPAA NIST Special Publications 800-52 requirement.

CLOUD SECURITY STANDARD

Vitalerter is using a secure account in Microsoft Azure cloud. The account complies with the GDPR and HIPAA Security Rule, which sets the standards for administrative, technical, and physical safeguards to protect electronic PHI from unauthorized access, use, and disclosure.

REDUNDANCY & BACKUP

All data is stored in Azure big data storage blobs and Azure SQL services, and is backed-up every few hours, and can always be recovered. Azure Storage stores multiple copies of data on different fault domains, and, by default, will replicate data to a backup data center (the geo replication feature can be turned off if desired).

STORAGE ENCRYPTION

All archived data is being encrypted. All data in encrypted in compliance with 45 CFR § 164.514(b) and separately stores the identifying/encryption key in an Azure service that falls within BAA scope.

July 10, 2017

VITALERTER
A vital leap to quality patient care

AUTHORIZATION

All services and data are only accessible by authorized personnel using unique, audited access controls. The system is using a HIPAA compliant cloud active directory system to manage access control, so only staff with relevant permission can access PHI data, limited to her permissions in the organization.

DATA ANONYMIZATION

Vitalerter stores only anonymized data, so developers of the system are unable to identify the patients. In some nursing homes, developers may become aware of general non-identifying patient details, specifically: age, gender and mobility level, but further identifying details are not stored.
Vitalerter uses the data for research and to improve the system, but for that we only use anonymized and aggregate views of the data.
Ideally, the nursing home should inform patients in advance of any research use of their personal data, but as the nursing home is sharing anonymized data they are not obligated to get consent from patients.
In some nursing homes, we ask for more information from the medical records of the patient. The essential point is that as long as we are not in a position to associate the data-set with an identifiable individual we are not required to get the patient's consent.
If at any point we should become aware of the patient's identity for research purposes, we should get the patient's consent for using the data, but currently the system does not store any such data.

DISPOSAL

All data is permanently disposed of when no longer needed. All SQL Server data is disposed after 30 days. All big data is archived in encrypted storage and disposed after 2 years.