CUSTOMERGAUGE INFORMATION SECURITY PROGRAM

HIPAA COMPLIANCE

Since 2008, CustomerGauge has been compliant with the strictest privacy rules, working under the EC Directive for Privacy in Europe, including Germany. IN this time we have developed a strict Data Security culture that is a very good fit for HIPPA and HITECH.

In December 2015, CustomerGauge announces that it is HIPAA compliant for the USA health market.

We aim for the very highest standards of data security and have implemented technical and procedural measures to ensure this.

Introduction

The Health Insurance Portability and Accountability Act of 1996 was enacted by the United States Congress and signed by President Bill Clinton in 1996. Title I of HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs. Title II of HIPAA, known as the Administrative Simplification (AS) provisions, requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers

CustomerGauge and HIPAA

Since 2008, CustomerGauge has been compliant with the strictest privacy rules, working under the EC Directive for Privacy in Europe, including Germany. IN this time we have developed a strict Data Security culture that is a very good fit for HIPPA and HITECH.

In December 2015, CustomerGauge announces that it is HIPAA compliant for the USA health market.

CustomerGauge supports Covered Entities (healthcare companies) understand the customer experience and feedback from indivduals and to keep private the “Protected Health Information” (PHI) of invidiuals in the course of contacting and surveying.

The methods used permit compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA). CustomeGauge acts as a Business Associate to Covered Entities. CusteormGauge has have adopted measures to ensure that it remains in compliance with HIPAA and any Business Associate agreements it enters into. Covered Entities can collect PHI in surveys with a HIPAA- Contract Extenstion and Business Associate agreement in place.

CustomerGauge compliance is under Title II of the act and relates to the
1, Privacy Rule
2. Security Rule

Privacy Rule

CustomerGauge supports Covered Entities (healthcare companies) wish to understand the customer experience and feedback from individuals and to keep private the “Protected Health Information” (PHI) of invidiuals in the course of contacting and surveying.

Our standard contracts ensure that we are compliant in that CustomerGauge uses “De-Indentified Data” In this sense we DO NOT STORE the so-called “18 identifiers” which include names, health insurance numbers account numbers etc. Instead, CustomerGauge uses a special identifier that links the customer feedback and results to the core data set of the “Covered Entity”

Should you wish to store any of the the “18 identifiers” in the PHI we use an extended contract, with a “BAA” – a Business Associate Agreement which covers the legal use of the PHI data.

Under the Privacy Rule, CustomerGauge has appointed a Privacy Official and a Contact Person through which individuals can request corrections to PHI and make complaints.

Security Rule

CustomerGauge is compliant under the administrative, physical and technical safeguards.

Administrative
- we have written procedures (see our attached policy)
- We have plans for breaches and contingencies.

Physical
- We are hosted on Amazon Web Services which have aligned HIPAA risk management program with FedRAMP and NIST 800-53, a higher security standard that maps to the HIPAA security rule.

- Access to heardware and software is strictly controlled.

Technical

- Encrypted data transmission and encryption at rest
- Firewalls with strict access
- USA based servers

We regularly audit the procedures and safeguard.

Key features:

- Regular risk assessments of systems to ensure that safeguards remain relevant and effective
- Screening, authorization, and training of CustomerGauge staff
- Data backup plans
- Disaster recovery plans
- Systems regularly monitored, updated, and patched
- Incident response plan that includes reporting of security incidents to affected covered entities
- All communications with CustomerGauge servers encrypted with SSL
- Automatic logoff: we time out user sessions after 30 minutes of inactivity.
- Logging of account access activity and modifications to survey data

Resources:

https://aws.amazon.com/compliance/hipaa-compliance/

https://en.wikipedia.org/wiki/Protected_health_information