General Data Protection Regulation

Frequently Asked Questions

Who is responsible overall within Aetna for Data Protection?

Aetna applies an integrated approach to privacy governance. The Group Chief Privacy Officer (based in the United States) is responsible for all matters related to data privacy and the Chief Information Security Officer manages security risk.

What will happen to Personal Data if the customer or member decides to withdraw from the service?

At the end of the policy customer data will, as contractually agreed or otherwise mandated by law or regulation, be returned, deleted or otherwise anonymised in accordance with Aetna's internal policies and retention schedules.

Who will ensure compliance with Data Protection requirements within Aetna?

Compliance with data protection requirements is a responsibility shared by every Aetna employee.

Contractually, is Aetna the 'Data Controller' in terms of the data Aetna process for its activities?

Aetna's obligations as a data controller or data processor in relation to the service it provides to customers are set dependent on the circumstances of each arrangement.

How will Aetna ensure compliance with GDPR?

Aetna will implement policies and procedures in accordance with the GDPR, consistent with our good faith interpretation of the requirements. Aetna is continuing to assess changes that may be needed in response to the GDPR. Aetna has established a project management discipline and governance structure to determine impact, assess and implement any necessary changes by the GDPR's effective date that may apply to processing of personal data related to coverage provided by Aetna.

Will customers have any additional obligations *vis* a *vis* Aetna regarding GDPR compliance?

Apart from assessing its own compliance requirements under GDPR, Aetna would expect customers to abide by contractually agreed privacy requirements. Specifically, this would include customers providing appropriate privacy notices to their end-customers/cardholders as well as obtaining any consents and permissions which enable Aetna to use such data for any agreed purposes.

To what extent will Aetna comply with Data Protection laws outside of the EU?

Aetna will comply with all applicable data privacy laws. More specific requirements may be set out in Aetna's customer contracts.

Does Aetna share or plan to share any personal data, including customer/member data, with third parties?

Aetna will only use and share personal data in order to provide its services and to comply with its legal, regulatory and contractual obligations. Aetna has implemented an expansive policy framework to manage personal data. This includes a Data Protection Policy, information security policies, Information and Classification Handling Policy and the Records Retention Policy. As a result, Aetna will only share personal data with its suppliers, business partners, regulators, law enforcement agencies, financial institutions, global payment networks or other third parties as necessary. As appropriate, Aetna will implement appropriate technical and organisational measures to protect personal data.

What procedures does Aetna have in place to handle disclosure of Personal Data to law enforcement agencies?

Law enforcement requests are handled by a dedicated team within Aetna who confer with the legal, compliance and other teams as necessary.

Is any customer Personal Data transferred outside of the European Economic Area ("EEA")?

UK and EEA customer data is stored in the UK. However, personal data may be transferred to an Aetna group entity within the United States and is transferred under the protection of model contract clauses.

What policies/documentation are in place to protect Personal Data when it is transferred outside of Europe?

As Aetna's key data processing infrastructure is located in the UK or EEA, its personal data is primarily stored here. To the extent Aetna processes any personal data originating from the EEA outside of the EEA, Aetna will implement all appropriate measures to ensure the security of the data and to comply with data privacy laws.

How does Aetna ensure the security of Personal Data?

Aetna is PCI certified for some of its key processing infrastructure and applies all necessary security measures, including encryption, tokenisation, access and other controls as part of its operations. Aetna has built a market leading security governance framework.

How will Aetna action requests for access, rectification or deletion of personal data?

Aetna will support its customers and members in responding to any requests they receive for access, rectification, erasure or objection to processing of their personal data.

Can copies of Aetna's data management policies (Data Protection, Information Security, Record Retention and Information and Classification handling) be shared with customers?

Aetna policies are generally not for external (customer) disclosure. However, a comprehensive overview about its data management policy framework is provided in the information security plan which can be shared with customers, subject to a non-disclosure agreement.

How can employees report data protection concerns?

Employees are able to highlight data protection concerns in a number of ways, including to line managers, the Group Chief Privacy Officer, the Information Security team, HR, Compliance or through a dedicated whistleblowing hotline.

How are data breaches and their reporting managed within Aetna?

Aetna has a dedicated security incident response process, managed by the information security team in conjunction with other stakeholders.

How does Aetna ensure compliance with GDPR and other data protection requirements by its suppliers?

Aetna has a supplier risk management framework in place which includes due diligence checks, contractual and other controls at the point of selection, on boarding and an ongoing supplier management lifecycle.

What training is provided to Aetna staff on Personal Data handling requirements?

Regular mandatory training is provided to all Aetna staff through integrated data protection and information security online modules and face-to-face training. Compliance with training requirements is monitored and tracked through Aetna's internal learning & development systems.

What mechanisms are in place to ensure effective implementation of Aetna's privacy policy?

In addition to online and face-to-face training, guidance on privacy and information security is available through dedicated intranet pages. Awareness of the data protection and information security policies in particular is highlighted throughout an individual's engagement, for example, through employee contracts and staff handbooks. It is further reinforced through privacy awareness campaigns incorporating quizzes, intranet communications etc. Further more detailed guidance is also available on Aetna's intranet and available to staff through a network of data privacy champions, which is embedded in Aetna's business units, enterprise level business and support functions and also form part of its data privacy governance framework.

How does Aetna ensure compliance with GDPR when handling US data?

Aetna will continue to comply with all applicable data privacy laws. Data that relates to US residents and holds no connection to the European Economic Area (EEA) will continue to be stored in the United States and will not be affected by GDPR. However, if there is any doubt as to whether there is anything to connect the data to the EEA, then each case will be individually assessed.

How does Aetna ensure security when transferring EU data?

The issue of transferring personal data out of the EEA is very broad. For example, if an Aetna employee in the US can access personal data located on an EEA server, or if data is emailed from the EEA to a US employee, this is classed as transfer of data out of the EEA under the GDPR. Aetna will only transfer personal data out of the EEA if it has a lawful basis for doing so and meets legal, regulatory and contractual obligations.

About Aetna International

Aetna International is committed to helping create a stronger, healthier global community by delivering comprehensive health care benefits and population health solutions worldwide. One of the largest providers of international private medical insurance, Aetna International serves more than 900,000 members worldwide, including expatriates, local nationals and business travellers. Its global benefits include medical, dental, vision and emergency assistance and, in some regions, life and disability. Aetna International also offers customised technological and health management solutions for health care systems, government entities and large employers to improve people's health, enhance quality of care and contain costs. For more information, see www.aetnainternational.com.

About Aetna

Aetna is a leading diversified health care benefits companies, serving an estimated 46.7 million people with information and resources to help them make better informed decisions about their health care. Aetna offers a broad range of traditional, voluntary and consumer-directed health insurance products and related services, including medical, pharmacy, dental, behavioral health, group life and disability plans, and medical management capabilities, Medicaid health care management services, workers' compensation administrative services and health information technology products and services. Aetna's customers include employer groups, individuals, college students, part-time and hourly workers, health plans, health care providers, governmental units, government-sponsored plans, labor groups and expatriates. For more information, see http://www.aetna.com/ and learn about how Aetna is helping to build a healthier world. @AetnaNews