The EU GDPR and Compliant Omnichannel in Pharma

Paul Battisson

mavens

The European Union General Data Protection Regulation (EU GDPR) was signed in April 2016 with the aim of both harmonising and strengthening legislation related to the protection of personal data for EU citizens processed by organisations.

As more channels have become available for communication, the regulatory burden for organisations has increased as they are required to not only maintain compliance but to do so across omnichannel experiences.

This new legislation has a large impact across all industries and sectors, but particularly within the pharmaceutical and healthcare industries where this intersection between regulatory requirements and a drive towards the omnichannel experiences that healthcare professionals (HCPs), patients and consumers now expect is already being felt strongly. Organisations must be compliant with these regulations but cannot afford to miss the opportunities presented by engaging with patients, HCPs and consumers in an omnichannel way to improve outcomes and provide much needed information. In this paper we will discuss the impacts this regulation will have on the drive towards omnichannel within the pharmaceutical space and how organisations can not only maintain compliance but also become omnichannel and scale their ability to engage in the future.

A typical digital consumer now owns three or more devices that are connected to the internet and expects to interact with an organisation using these devices.

Over the past 20 years there has been a rapid growth in both the number of available channels for an individual to communicate and the way people interact with technology. A typical digital consumer now owns three or more devices that are connected to the internet[1] and expects to interact with an organisation using these devices as well as the channels they enable such as social media or chat. In the pharmaceutical industry, this change has been most sharply highlighted by the decline in the number of sales representatives an organisation has[2] as well as the time and access these representatives have with HCPs.[3] The individuals that a pharmaceutical organisation interacts with, be they an HCP, patient, or consumer, are all transitioning to a world with many devices and channels in their personal lives and expect their interactions with pharma to be no different.

For pharmaceutical organisations, one of the greatest challenges in delivering this connected experience is ensuring consistency and connectivity across brands as well as channels. Organisations have multiple brands and therapeutic areas, each

[1]https://www.globalwebindex.net/blog/digital-consumers-own-3.64-connected-devices

[2]https://www.wsj.com/news/articles/SB10001424052748703702004576268772294316518

[3]https://www.zs.com/-/media/pdfs/ph_mar_wp_afm_acm_2016_es_v4.pdf?la=en

of which has built up its own series of point solutions and data sets for providing information and services. The GDPR specifies that an individual's data be accurate and kept up to date as well as easy to report upon for the data subject if they request it. Having a series of disparate point solutions makes this extremely difficult to manage and maintain with confidence, risking non-compliance.

The challenge for organisations then seems to be threefold; firstly, how can a pharmaceutical organisation provide omnichannel experiences for HCPs, patients and consumers? Secondly, how can they do this whilst maintaining compliance with the GDPR regulation? Finally, how can technology support scale as they add further channels and brands in the future? In this paper we will discuss some of the key challenges for organisations.

Accurate and Up-to-Date Data

Within the principles relating to the processing of personal data, the GDPR states that "personal data shall be accurate and, where necessary, kept up to date." As we discussed above, many organisations are still working with data siloed in multiple systems. The data is disconnected, making it difficult to maintain accuracy when the data subject changes their information. It is possible for organisations to put processes in place to make this easier, but this can be a timely and costly endeavour as the mapping of data between these many systems, ensuring compatible connectivity and even collating a taxonomy of these solutions, requires the involvement of many parties and teams often geographically spread.

By maintaining the data multiple times in different silos, organisations remove their ability to obtain a complete and accurate of an individual.

From a strategic perspective, data silos also make it difficult for an organisation to deliver services in an omnichannel way to HCPs, patients, and consumers. In his Omnichannel Hexagon, Rasmus Holland[4] defines "Customer Recognition & Permissions" as one of the six key disciplines of omnichannel marketing as it enables an organisation to begin communicating with an individual on a more frequent and direct basis rather than waiting for an individual to contact the organisation themselves. Storing and managing this data is the backbone of providing personalised services and, by maintaining the data multiple times in different silos, organisations remove their ability to obtain a complete and accurate profile of an individual.

[4]Make It All About Me And I'll Buy It! by Rasmus Holland, Saxo Publishing, December 2015

It is therefore suggested that an organisation create a single enterprise store of identity that enables an individual's data to be managed and maintained within a single location. Not only will this ease the burden of ensuring that data is kept accurate, but also enables the organisation to build a more complete picture of an individual for use in the provision of omnichannel services.

Transparent Reporting

Siloed and disconnected data makes it difficult for organisations to keep data accurate, whilst data connected in a single store enables a much more complete view of the individual to be created and allows data to be reported upon more effectively. This is again another key component of the new legislation, with organisations required to provide the data in "a concise, transparent, intelligible and easily accessible form, using clear and plain language."

Pulling such information together from multiple data silos has an inherent risk that certain data is missed or not correctly identified and reported, even if processes are put in place to maintain data synchronisation and referencing. Further to this, the legislation requires that the report be provided within one month of the request from the subject, with the ability to extend this timeframe by a further two months where necessary, taking into account complexity and number of requests.

When an organisation stores the data using a single enterprise identity service, they are able to produce such reports faster, lowering the organisational and financial burdens of such requests. This ensures their regulatory compliance and also enables the organisation to build trust and rapport with data subjects through open and responsive communication to requests.

When an organisation stores the data using a single enterprise identity service, they are able to produce such reports faster, lowering the organisational and financial burdens of such requests.

This reporting meets regulatory requirements and allows personalisation of communication. The organisation has a more accurate and relevant picture of a data subject, mitigating the possibility of sending information that is irrelevant or unrequested, for example articles regarding rheumatology to an HCP who specialises in oncology or sending an email to a patient who has opted out of such communications.

Consent Capture

With regards to the management of opting in or out of communications, the legislation is clear; an organisation must demonstrate readily that consent has been provided by a data subject and that it is presented in a clear manner. The regulation also states that the data subject should be able to withdraw consent as easily as they can give consent. Often this is obfuscated behind a lot of processes, sometimes because organisations wish to make it difficult for individuals to remove consent, but more often than not because the way in which the consent data is stored is not conducive to simple management and maintenance.

For example, an HCP may have consented to receiving emails from an organisation around her work in the cardiology space and as part of this is receiving information around a "My Healthy Heart" initiative. The HCP has decided she wants to keep informed about work in the cardiology area but not the "My Healthy Heart" initiative as it is not of interest to her. How does the organisation handle this request? Is the consent for this stored in a single place or in multiple systems? Is the consent managed on an initiative level or is it simply opt-in or opt-out globally for such communications? If the organisation has multiple silos of identity information how can we be assured that the organisation complies with the opt-out across all these solutions?

An organisation must demonstrate readily that consent has been provided by a data subject and that it is presented in a clear manner.

So how should this consent data be stored to enable effective management? Again if we have a single identity store for the enterprise, we can manage consent alongside this single identity and provide a more rational and easy way to work with the store of data. Across channels this enables us to to proactively validate whether our users have consented to particular forms of communication and allows us to dynamically engage with them. We must make this data readily available via simple to use APIs for systems to both consume and update the consent data as needed using our identity information.

Additionally we must consider what we mean by consent and how best to store this to enable flexibility and control from the perspective of both the data subject and the organisation. For many organisations, consent is seen as a one-dimensional piece of data for an individual, they have either consented or they

have not in what is often called "enterprise wide consent." This one-dimensional view leaves virtually no flexibility for either the data subject or the organisation though; they are either able to be interacted with or not and personal preferences and opportunities for engagement are missed. Instead consent should be viewed as a multidimensional piece of information for a particular user which can also vary over time.

Firstly, we need to extend our simple view of binary consent into one where we are tying a particular set of consent language to a specific initiative we are undertaking, for example the ability to contact an individual via email to the "My Healthy Heart" initiative. With this approach the individual data subjects understand what they are consenting to, so that we are compliant with regulations and the organisation has a simple and effective way to understand what consent has been given for different channels. By doing this we have switched our original one-dimensional consent model to a two-dimensional model of preference and consent language that allows us greater regulatory compliance and control. We can then further enhance this model by requiring that our consent be attached to a particular address, whether it is a physical address, phone number or digital address such as an email or smartphone app, creating a three-dimensional consent cube of initiative, language and channel/address. By including this additional dimension we have again improved our ability to be compliant with the regulations and enhanced clarity to our data subjects, whilst further improving our ability to capture and manage consent for different channels and brands.

We briefly mentioned the concept of time for consent as well. Using our updated consent cube model, we can capture at a granular level when consent was granted or revoked, but must also anticipate change in regulatory needs, wording of the agreed consent language and legal requirements for the consent to be recaptured or reaffirmed. Again our new model makes this possible by enabling us at a granular level to set renewal dates on the consent we have captured so that we may prompt our user to reaffirm their consent and maintain compliance.

Using our updated consent cube model, we can capture at a granular level when consent was granted or revoked.

Right to Be Forgotten

Within the legislation, the data subject now also has the right to ask for complete erasure of the data related to them where they have due course to do so. Reviewing the model for identity and consent that we have constructed, we can see that by maintaining a single identity for an individual alongside the consent that individual has provided, we have a simple way of ensuring that, when a data subject requests their data be removed, we can do this and validate the removal within the system.

If instead we were to be using our older more siloed model of identity and consent management, we would have a greater level of difficulty in processing such a request as multiple systems would need to be queried, cross-referenced and updated to ensure that the request had been fulfilled. We would also face the risk that an individual's data was not completely removed as it may still remain where it has not been correctly identified or linked. Not only will this lead to non-compliance, but from a practical perspective increases data bloat as incorrect or irrelevant data is being stored, reducing the accuracy of analytics and knowledge.

Our New Omnichannel-Ready Model

We have now built up the concept of a new data model for managing identity and consent in a way that is GDPR compliant and enables us to meet these new regulatory needs whilst reducing our workload and burden. We have transitioned from a siloed structure of many disparate identities across the organisation, each with their own consent stores and concepts, to a single identity.
We can now store consent against this identity in a granular and structured way that enables us to have a clearer view of the individual as well as ensure that we can be both transparent and compliant in all of our engagements.

This model also enables us to begin engaging more effectively in a truly omnichannel way, where all of our interactions and engagements are seamless and connected for our patient, HCP or consumer. Using this new model we can begin to manage preferences, connect experiences and understand how the individual interacts with an organisation in a

MAVENS CUSTOMER INTERACTION MANAGER

Mavens Customer Interaction Manager helps you build real, enterprise-level relationships with your HCPs, consumers, and patients. Our platform helps you manage communication across different channels so you communicate in a way that's relevant, customized, and branded.

more complete way rather than having a set of disjointed and disconnected interactions. This new engagement model is not just limited to the obvious channels such as web and email, but also more timely and relevant channels such as connected conferences kiosks and mobile applications.

Historically the pharmaceutical industry has had a focus around brands out of which these siloed data sources and applications have grown, however the rise of patient and customer centric services have led to the need for this model to be re-evaluated for a more connected, omnichannel approach. For patients this means better education, provision of help and timely information to help them better manage their condition. For HCPs, relevant and timely materials, a more transparent and trustworthy engagement model and a unified experience.

Summary

We began this paper by focussing on some of the core challenges facing pharmaceutical organisations from the upcoming GDPR and discussing ways in which we can mitigate these through an updated approach in organising and managing our identity and then consent information. We then saw how this new data model not only ensured that organisations had the ability to be compliant with the new regulation, but actually enhanced the ability of an organisation to be able connect and engage with an individual in a more seamless omnichannel way, enhancing the organisation's ability to connect and engage.

ABOUT THE AUTHOR

Paul Battisson is a Technical Architect with Mavens, based in the UK. Over the past 15 years he has delivered solutions across a wide range of sectors including many highly-regulated industries. He has spoken at a number of healthcare industry and technology events on topics as diverse as machine learning, virtual reality, patient services and omnichannel marketing in pharma.

ABOUT MAVENS

Our mission is to elevate healthcare worldwide by connecting people to cures through cloud technology and trusted partnerships.

Mavens implements software that transforms the way organizations engage with healthcare professionals, patients, and consumers. Our strong relationships with Salesforce and Veeva help us deliver with unmatched speed, innovation, and partnership.