Hospify

Securys

# Security FAQ

August 2020

# Why is Hospify Secure & Compliant?

## Platform architecture overview

Hospify was designed in close consultation with the Information Commissioner's Office to ensure compliance with both UK data protection laws surrounding health data and the GDPR. The platform's architecture is specifically designed to significantly reduce the potential for security breaches and legal liabilities around patient data access requests.

## Hospify Mobile App

### 1. Text messages

Hospify encrypts and delivers messages from phone to phone, using real-time PubSub servers and a SQL database for message queuing and longer-term message storage, when required (see Web App section, below).

Data in transit uses TLS 2048-bit encryption and is never stored in the message transit servers for more than 72 hours even if delivery fails. The SQL message queues will store messages that have not been delivered immediately for 72 hours to attempt redelivery; after 72 hours, if delivery has not been achieved then the message is deleted, and the sender is informed that delivery has failed.

Messages are automatically deleted from both sender and recipient phones after 30 days. Please note that the deletion process relies on a user opening and using the app. In theory if a user doesn't use the app then the messages remain. In this case, to access the encrypted messages a bad actor would both need to gain "rooted" access to the device and the encrypted message, and access to the private keys held in the phone's secure storage hardware, which isn't supposed to be possible even with a "rooted" device.

Hospify's user database servers are kept entirely separate from the message transit systems and the keys required to decrypt the message are stored separately from the encrypted data itself.

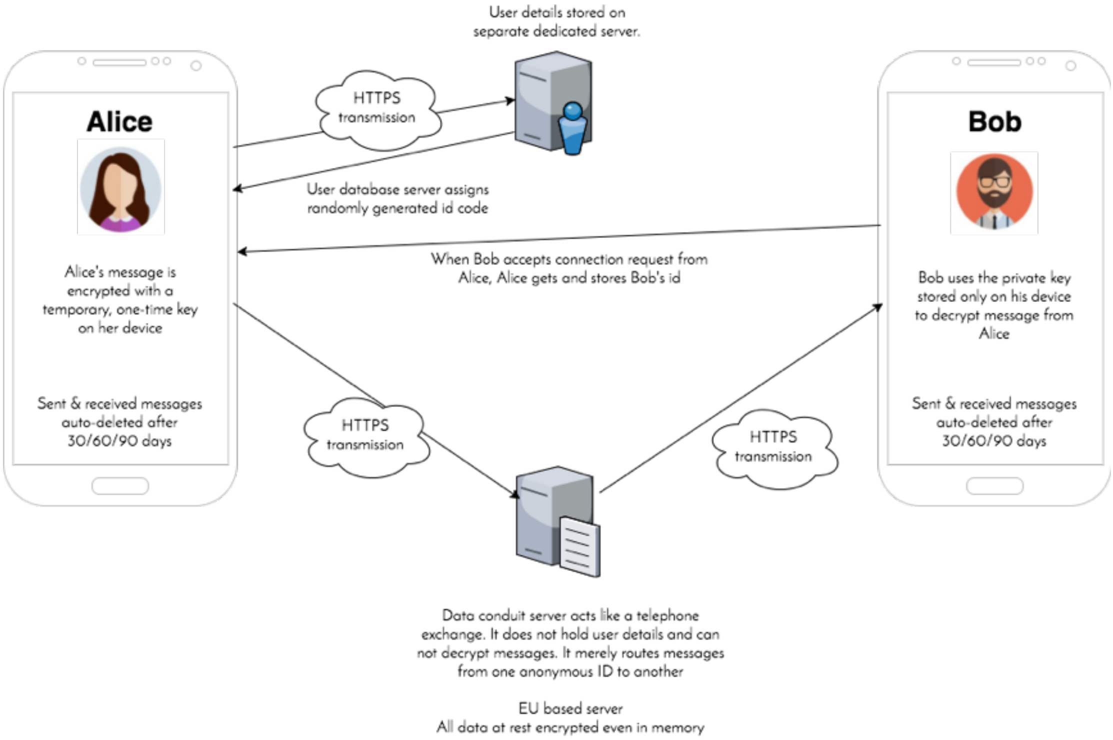
Hospify's servers are exclusively based in the European Economic Area, ensuring that all messages stay within that geographic zone. Similarly, the premise behind Hospify's approach to security is to keep all private data on the user's device and to do all encryption on-device before transmission.

On device the hardware security features are used to store sensitive information such as keys. We have implemented all standards using ephemeral keys to provide perfect forward secrecy too. AES256-bit encryption is used for data encrypted at rest.

PKI keys are stored in the phone's secure hardware environment, using Apple KeyChain for (iOS), or the class CryptoControl (Android). Any other data is encrypted at rest again using AES 256-bit encryption. The app has its own PIN entry/biometric login screen and so does not rely on a user setting a PIN for the device itself. On device data is purged after 30 days - users cannot keep messages in Hospify any longer than that. None of the message content is shown in home screen notifications, which just tell you that you have a secure message in Hospify from a named individual but offers no further information about the message contents.

Hospify uses an Elliptical Curve Private/Public key infrastructure and AES 256-bit for the symmetrical encryption of the derived key. This design is driven by the best-practice standards and is very similar to the way https now works. All of the encryption takes place on the user's device.

The data flow model displayed below illustrates this:


User details stored on separate dedicated server.
HTTPS transmission
Alice
User database server assigns randomly generated id code
Bob
When Bob accepts connection request from Alice, Alice gets and stores Bob's id
Alice's message is encrypted with a temporary, one-time key on her device
Bob uses the private key stored only on his device to decrypt message from Alice
Sent & received messages auto-deleted after 30/60/90 days
HTTPS transmission
HTTPS transmission
Sent & received messages auto-deleted after 30/60/90 days
Data conduit server acts like a telephone exchange. It does not hold user details and can not decrypt messages. It merely routes messages from one anonymous ID to another
EU based server
All data at rest encrypted even in memory

## 2. Picture messages

For communicating picture messages, the app operates a dedicated picture server. Full resolution and thumbnail versions of the picture are encrypted and then uploaded to the server where they are kept, stripped of metadata, for a maximum of 32 days while awaiting download by the authorised recipient(s). Access to encrypted files is limited to authenticated users, and only the intended recipients have access to the decryption keys for each picture.

Pictures are taken by a camera accessed from within the app and are stored within the app so that they do not get inadvertently shared in a non-compliant fashion by the user's phone's picture cloud storage function. Screenshots are suppressed on Android phones (this functionality is not currently available in Apple iOS), to further discourage export of information from Hospify.

## Hospify Web App

Hospify's Web App provides users with access to their messages via a web browser; as a result, it does not store any user or message data on the device as it may be shared with other users.

When sending messages, the Web App uses a Hospify API to encrypt the messages for each recipient and then the messages are sent directly to recipients using the same messaging transit system used by the Mobile App. As above, a copy of each encrypted message is stored in the central database.

When receiving messages, the Web App downloads encrypted messages from the central SQL database (access to messages is strictly limited to the intended recipients). Messages are then decrypted via a Hospify API before being displayed to the user. Messages are stored in the SQL database for a period of 12 months by default. Longer storage times are available as an additional premium feature.

In transit, text messages are encrypted as described above for the Mobile App. Picture messages also operate in the same way as described above for the Mobile App.

It is important to note the encryption and decryption algorithms work the same way as for the mobile app, through symmetrical keys but that encryption and decryption do not occur on the device itself. Messages are encrypted for each recipient and It is only possible to decrypt a message using the recipient's private key. However, a key difference from the Mobile App is that since the private key cannot be stored on the device, it is stored in a cloud database which is kept isolated from any other message or user data. This private key is not transferred to the browser and can only be accessed or used by the API server.

## Hospify Hub

The Hospify Hub is an online admin portal that enables organisations to manage their users and groups; it also allows them to broadcast messages to "Audiences" (i.e. tagged segments of their user base).

The Hub is accessed via a web browser and does not store any data on the device. It only provides access to user data via a Hospify API and is not able to access any messaging data.

Broadcast messages sent from the Hub are not encrypted and are stored in a database. Broadcast messages are not intended to carry sensitive information or patient identifiable data. Access to broadcast messages is limited to the intended recipients.

All data in transit to and from the Hub are protected by SSL and by a multi-tenant authentication system.

## Version control

Hospify operates a robust system of version control over all aspects of its code base, to ensure that non-approved code cannot be released to a live production environment.

1. System of gated commits in place; no code can be committed to release branch without sign-off by CTO or specified senior developer
2. All testing is done on a separate branch that has no access to live data
3. Hospify's Information Security Policy, induction procedures and Staff Handbook specify that executives/suppliers/employees managing release code should be specifically alert for malicious code inserts.
4. We use git for source code version control. Separate branches are maintained to ensure release code is specifically audited and review prior to a production release.

## Testing activities

Within the mobile app and desktop client app we use standard and open standards cryptography within our product. The cryptography functions make use of the Microsoft core .Net libraries and the BouncyCastle (http://www.bouncycastle.org/csharp/) cryptography library. The Bouncy Castle library is a well-respected library first released in the 1990s and with the latest update on 31st January 2019. It has gained FIPS-140 (https://en.wikipedia.org/wiki/FIPS_140) certification and has extensive unit testing of its own routines.

In addition to the Unit Testing provided by the third-party libraries we use we conduct our own testing.

Our own HKDF (https://en.wikipedia.org/wiki/HKDF) tests against the RFC 5869 standards (https://tools.ietf.org/html/rfc5869) for SHA-256 keys. Those are the only ones we use.

We also carry out tests of our public / private key generation algorithms to ensure consistency and validity of the public / private key pairs, and testing of our implementation of our routines that conduct encryption and decryption of data against both known good input and malicious inputs to the algorithms.

Our server infrastructure is hosted within the Amazon (AWS) system and benefits from their testing environment with regards to the hosting of code and delivery of data via an API with protections against attacks such as DoS.

Our own code base for the server is thoroughly unit-tested. We have in excess of 2000 unit tests covering cryptography, data input / output validation, database consistency and edge case testing for malicious data inputs. Approximately 50 tests cover functional testing of the API endpoints.

In addition, we have developed a separate application named Hospify Probe that is only deployed internally. It serves as a preliminary testing platform for any new code and any major alterations to the networking and communication layers with the app. We maintain a number of live Probe instances to monitor our network and ensure consistency of our service.

We use the Gitflow workflow as described in https://www.atlassian.com/git/tutorials/comparing-workflows/gitflow-workflow. This means our release code is kept within the master branch and a development branch (dev) is used for feature integration and testing prior to release.

JIRA is used as a project management tool and all tasks are assigned a JIRA ticket with translates into a feature/* branch with our Gitflow. We also maintain a hotfix/* branch folder for minor bug fixes.

## Processes for accepting and responding to technical faults from end users

End users can report issues using the "Feedback" feature in the Hospify mobile app itself, via our website, or using the email support@hospify.com. If the issue cannot be resolved directly by our support team, it is filed to our Jira development backlog, where it is picked up by our development team as part of their agile work cycle.

Issues that affect multiple users or require a significant amount of work are recorded in our ISO27001 Jira project management tracker, along with any data-related incidents and resolutions This log is then included in our formal company internal audit and forms part of our ISO Business Management System.

## Rollback process

As part of the GitFlow described above we also maintain tagging to keep track of our release builds. Frequent small commits to the code base allow reversion and rollback in case of a regression. And if a full rollback to a previous version is required then tagging allows us to identify the last known "good" commit.

Proactive monitoring running of systems and system components to automatically identify faults and technical issues

We have built our own modular messaging test rig, called Probe, that allows us to continually stress test the actual messaging component of the Hospify platform independently of the front-end app. Using Probe we can also test all updates and changes to the message transport systems, before releasing them in the user-facing app.

We use a platform called Lumigo to monitor our AWS lambda stack. The Lumigo platform inserts an AWS layer in front of all lambda functions in order to track execution times, performance, memory usage and error conditions. Those are then reported in a dashboard available for inspection by Hospify staff. There are integration directly into JIRA, however, they are yet to be implemented.

Internal monitoring tools have been developed to monitor the messaging stack. These run on a scheduled basis and are deployed to Heroku instances. They provide us with metrics on message deliverability and performance. They will allow us to identify messaging layer issues occurring server side. Note they do not monitor client side (e.g. mobile app) performance.

Ensuring continued availability Hospify operates according to the precepts of its ISO27001 Disaster Recovery Policy, which stipulates that:

1. The company will use redundant third-party cloud-based services whenever practical, to minimise the risk of physical catastrophe interrupting the continued operations of the business.
2. A list of potential alternative third-party cloud-based services to those in use shall be maintained by the CTO, and regularly reviewed by senior management. All development and operations shall abide by the principle of exchangeability, with regard to these services, which is to say, shall be designed in order to allow third-party services to be replaced as easily as practical. A record of provision and exchange reviews is held in the Hospify Asset Register.
3. All operational and legal documents shall be held in electronic format on the Hospify Google Drive, which shall be installed and regularly synced over at least two computers and backed up once a week to a securely single AES256-encrypted hard-drive, protected with a 12-digit password, by the CEO.
4. The password to the encrypted hard-drive shall be known to both the CEO and the CTO and that knowledge reviewed in an audited face-to-face meeting every six months (the audit being the record at the end of this policy).
5. Copies of the offline cryptographic locker holding the live keys required to access the Hospify servers along with all other passwords to online services regularly in use are held by the CEO, CTO and Internal Auditor.
6. The password to the offline cryptographic locker shall be known to both the CEO, the CTO and the Internal Auditor and that knowledge shall get reviewed in an audited face-to-face meeting every six months (i.e. the BMS management review).
7. A live test of the backups and redundancies shall be done annually, emulating denial of service to key staff, emergency access to key codes, and emergency access to code base backups (the audit being included in the record at the end of this policy).

## Processes for decommissioning the product and dealing with any retained identifiable data

Hospify is deliberately architected according to the data minimisation principles specified by the General Data Protection Regulation. All textual message data is deleted from its servers after 72 hours, and all picture message data is deleted from its servers after a maximum of 32 days. Both textual and picture data are automatically deleted by the end user's mobile app after 30 days.

As a result, should Hospify ever be decommissioned, the company can guarantee that all user-generated data is completely removed from both the company's servers and end users' mobile apps after no more than 30 days, whether users delete the app from their phones or not.

The only other data Hospify holds is user profile data both for the user contact directory and for each Hospify Hub web portal (held on a GDPR compliant SQL servers). Should the platform be decommissioned, these servers and their backups would be deleted immediately, and users would have no way of accessing the data subsequently, as it is not possible to create backups or exports of this information.

## Processes for dealing with any retained identifiable data in the event that an individual should stop using the platform

Should a user stop using Hospify, they can simply delete the app and email our support team requesting that they be removed from the Hospify directory (held on a GDPR-compliant SQL server as noted above). This is a simple procedure and has already been carried out multiple times).

# Other Frequently Asked Questions

## Why not just use WhatsApp?

WhatsApp is a great tool that delivers billions of messages a day to its 1.5bn users around the world with incredible efficiency. But that utility does not make it appropriate for communicating in situations where one user has a legal and social responsibility to safeguard another user's privacy, and that's the case in health care.

There are a whole variety of reasons that WhatsApp is not – and in its current form can't be – a compliant messaging tool that is appropriate for use by healthcare professionals. We're going to look at them here, in turn.

### 1. Where the data are held

Under the EU's General Data Protection Regulation (GDPR), which was enacted in UK law in May 2018, requires you to take appropriate measures and adopt safeguards when transferring and storing the data abroad, which complicates matters as Whatapp stores its data all round the globe.

Why does this matter in health care? It matters because users of a health care messaging platform are likely to include doctors and nurses, and they tend to talk about patients. As soon as you mention a patient by name in a text message and add any details about their condition, then you're holding personally identifiable data about them which, given the context, is likely to include sensitive health data.

Article 9 of the GDPR defines sensitive data as ' personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership and the processing of genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.' Article 9.2 (h) of the GDPR and Schedule 10 (8) of the Data Protection Act 2018 contains a condition for those who work in health and care: they are allowed to communicate and store details about patients without asking express permission, as long as they're doing it in the course of delivering their care.

To take advantage of this condition, though, UK & EU-based health care professionals need to use a communications system that handles data in a way that is otherwise compliant with both the GDPR and the information governance rules of their health care employer. WhatsApp isn't compliant, simply on the basis of the geographical location of its servers.

## 2. Access to the data

The second problem is to do with accessing this personal information once it exists. WhatsApp messages are encrypted both in transit as they travel around the internet and at rest on their servers. But storing them like this creates problems. If you're a doctor and you've chatted with another doctor about one of your patients – to get some advice or a second opinion about their condition, for example – then you don't own that data. Your employer, i.e. the hospital or surgery where you work, owns it instead, even if it is on your phone. Your employer is therefore ultimately responsible for it and – by law – has to be able to hand it over to the patient if the patient asks for it, which patients can do by issuing a fairly straightforward data subject access request.

As we've seen from cases like the 2017 Westminster knife attack, when WhatsApp refused to hand over the content of the attacker's messages to the Home Office on the grounds that even it couldn't de-encrypt them, getting access to WhatsApp messages is tricky. This creates a paradox. In the case of the patient, the law says that the hospital has to hand them over. But if they're on WhatsApp it cannot hand them over, because without de-encrypting them it can't work out which ones they are. So because a doctor talked about a patient on WhatsApp, and that patient issued a data subject access request, the hospital is now in data breach twice over: because the messages are being stored on a server outside of Europe, and because it cannot de-encrypt the messages and hand them over.

## 3. Photo Sharing

Another issue WhatsApp faces is the way it stores photos. Have you ever received a picture on WhatsApp? Have a look in your phone's main photo gallery. The picture will most likely appear there, as well as in WhatsApp itself. This is because nearly everyone's devices automatically backup such pictures to cloud services that are likely to be geographically located outside of Europe, and often shared with other members of your family. Even if you switch this feature off, Apple and others may be able to switch it back on without your knowledge.

## 4. Home screen notifications

Another non-compliant feature of WhatsApp is the home screen notification. You do have the option to switch notifications off for WhatsApp messages, but almost no one does; it is convenient for users to see that they've got a new message, after all. The trouble is that the notification contains a snippet of that message, available for anyone within viewing distance of your phone to see. This potentially exposes sensitive patient data to prying eyes, breaks most employers' "clean screen" policies, and is therefore another reason that WhatsApp isn't compliant when it comes to health care information governance.

### 5. Secure access

While it is possible to set a separate PIN code or fingerprint lock on the WhatsApp app itself, this is not enforced by the app. If this is not set up and your phone is stolen or lost or has been left unlocked for any reason, then there's nothing to stop someone getting access to your entire message history.

### 6. Data exploitation

Then there's the question of what WhatsApp is really doing with your data. In early 2018 Google struck a deal with WhatsApp (which itself is owned by Facebook) to allow WhatsApp users to back up all their chats and photos to their Google Drive accounts without impinging the 15GB free storage limit set on those accounts.

Now, this seems quite an odd thing for Google to agree to, given that Google and Facebook are major league competitors for online advertising spend. Would Google do such a deal out of the goodness of its heart? Presumably it's getting some kind of value out of storing all that content which, despite being encrypted, would still be laden with all kinds of associated metadata that the search giant could use to improve its profile and advertising of, yes, dear reader: you.

In addition, WhatsApp is to start serving advertising of its own in 2020 as confirmed by Facebook at the annual Marketing Summit in the Netherlands. In June 2018 WhatsApp's original founders Jan Koum and Brian Acton resigned from the board of the company in protest at Facebook's plans to introduce marketing and advertising into their chat app – which they'd faithfully promised from the service's inception would never be allowed. They were serious, too – their resignations cost them around $1.5bn in forfeited share options; a hefty price to pay for sticking to their principles.

This means that Facebook's coming after the data you expose through WhatsApp in order to allow businesses to target you. And if the data you're exposing is information about someone else's health, then that's a major problem and violation under the GDPR and UK data protection law.

### 7. Security

People often think that WhatsApp is secure because its messages are encrypted. But it turns out that it's not that secure at all. A bunch of white-hat hackers called Check Point Research  found that WhatsApp's QR-code feature, which allows a user to route his or her account via a laptop or desktop computer for ease of access, contains a vulnerability that allows an attacker to intercept group messages, change the identity of the sender, alter the text of replies to the group, and send private messages that go public to a group when responded to – all of which open the app to abuse and compromise privacy.

## Does Hospify sit behind an additional passcode? What's the time-out?

Yes, there is a separate app passcode. There is no time-out feature while the app remains open in the foreground. The app can be backgrounded for between two minutes and 24 hours before requiring the PIN to be entered upon reopen (user configurable). Device sleep pushes the app to background and re-entry of PIN is required on opening. There are options to replace the PIN with in-phone biometrics, if required (user configurable)

## How is user identity validated?

In the free mobile app, user identity is validated against certified email address, and professional users are encouraged to enter workplace details in order to be more easily found and identify colleagues.

For the paid web app, user identity is validated against credit card details by Hospify or by a data controller via the Hospify Hub.

Hospify intends to add additional validation checks for clinicians to further authenticate their identities in late 2020/early 2021. The first of these is likely to be validation against the NHS Identity API, for which we have applied for access.

Connections and communications within Hospify are entirely permission-based – a user can only connect with another user by sending them a contact request and having the recipient approve it, approval that can be revoked at any time. Our End User License Agreement specifies that users therefore need to be aware that they are responsible for only approving requests from people whose identities they are certain about.

In the real world, of course, people have the same name and identity theft, or impersonation is an online issue that has yet to be satisfactorily tackled by any company or government. For this reason, the Hospify Hub offers the option for Hub administrators to badge people as "Verified Users". A person marked as Verified by a Hub administrator will have the logo of that Hub appear alongside their name in the Hospify directory, so that another person searching in Hospify can see that their identity has been validated.

## How secure is the data on an individual's phone?

Very secure indeed. All data is completely sandboxed within the app, encrypted, and protected by the 6-digit PIN code, which you have to enter each time you use the app. No message content is shown on home screen notifications, all data within the app is automatically deleted after 30 days, and photos taken within the app are not shared with your phone's photo gallery (users may import photos from the gallery into the app, but not vice versa).

Hospify also disables screengrabs on Android to discourage people from exporting data it would do this on Apple too, but Apple do not currently allow the screenshot feature to be disabled by individual apps.

## Can I remote wipe my phone if it's lost or stolen?

Remote wipe is a function provided by the Apple or Android operating system by their enterprise setups. Hospify user accounts are only held in-device, they are covered by the operating system remote wipe function. There is no need for a remote wipe of the server storage, as there is no server storage. Hospify deletes all text messages from its servers after 72 hours of sending, and all pictures after 30 days. As Hospify is PIN code protected in-device, much like a banking app, it is secure if the device is lost or stolen even if it is otherwise left unlocked.

## Why is holding patient data on a device secure? Why is this better from a data security point of view than storing the data in secure servers?

Holding data on the phones rather than a cloud-based server makes that data more secure - it's harder to hack an individual phone than it is to hack a server, as you generally have to actually have the phone in your possession, making it almost impossible to hack phones at scale.

## Why is storing data in phones rather than on servers better from a compliance point-of-view? Under the Freedom of Information Act (FOI) or in the case of a Patient Subject Data Access request, any information stored could be subject to disclosure.

Hospify's "minimum viable data" architecture is designed specifically to mitigate liability around FOI or patient subject access requests (see the "Retention" section, above). The rule of thumb here, as explained in Section 52 of this ICO document, is that data that has been deleted does not have to be handed over.

Data in a Hospify conversation that should have been recorded into the patient record in the course of a clinician's work should be copied there using normal channels, just as it would be after a relevant phone call. This does not require the information to be copied verbatim; a summary of the salient points is sufficient (just as doctors are not required to record all phone calls, they have concerning each patient).

Where data is still live and contested, as it might be before it has been deleted from someone's phone under Hospify's 30-day auto-delete policy, the key thing to understand is that a provider of secure messaging in the health sector, Hospify's legally defined role is that of data processor. The individual hospital Trusts whose staff are using Hospify will have the legal role of the data controllers (for definitions of these terms as defined by the data protection act see the ICO website).

Trusts and other health institutions (GP surgeries etc) are the data controllers of any data that their employees might send via Hospify regardless of whether or not they directly procure Hospify's services, simply by being the employers of the people who'll be using it in the course of their work (even if those employees have the app on their own phones and pay for it with their own money).

Bring Your Own Device (BYOD) policies mean that hospital staff can own the device and software they use at work. These policies do not mean that staff therefore own the data on that device, if it is generated in the course of their employment. The Trusts own that data. It also means that staff who use non-compliant messaging services in the course of their work are technically in breach of their employment contracts, as they are not complying with their employer's duties and responsibilities as data controllers.

In the case of legal problems, Trusts can therefore ask employees to unlock (and therefore de-encrypt) any data that is held within Hospify on their phones. Even if Hospify held the data on a server, it wouldn't be able to unlock that data, as it is encrypted – and only the end user holds the key. By holding data in-phone only, the legal requirement for Hospify to de-encrypt and hand over the data is removed, but the Trust is still able to access live data by asking an employee to hand over their phone and in-app PIN code. For an employee to refuse to do this would result in a disciplinary and, in certain circumstances, is also a criminal offence.

## I get all that, but I still think it would be useful for there to be 'super-user' access to all groups so that information can be gathered. Is there any specific facility for this or would this be a case of adding a 'super-user' account to every group?

This is possible using the Hospify Hub, the paid version of Hospify. The Hub provides "a super-user" online administrative portal that allows authorised admins to set up and coordinate their own community of Hospify mobile app users. The admins can set up and audit official user groups, broadcast messages to specified sections of their community, and give their members access to the Hospify Web app, which enables group audit and moderation, long term message storage and export of data into other applications.

## Why doesn't Hospify integrate with the Electronic Patient Record (EPR)?

Hospify does not currently handle patient records or integrate with the EPR. Hospify is not required to provide access to a single point of record - that onus is on health data *controllers*, and Hospify is a data *processor*.

Patient records are the responsibility of the NHS and are held and communicated only within the NHS's secure N3 network, which is specifically designed for such purposes. Hospify is not proposing to hold or communicate patient records, nor is it planning to gateway with the N3 network or third party EPRs. This is something we have investigated but have rejected on the basis that it would be:

- Technically challenging to implement and expensive to support, and would substantially increase the price of the service
- Different in different situations – the EPR is not one technology but a shifting collection of technologies, some of which are commercial applications in their own right and often charge for full access to their integration APIs.
- Restrictive regarding Hospify's options for server provision
- Unnecessary technically, as it wouldn't facilitate Hospify's service in any significant way
- Unnecessary legally, as neither NHS IG, UK Data Protection nor GDPR require all message transmissions to be stored in the EPR. Noting the fact and salient details of a Hospify communication using existing interfaces, as a clinician would do for a relevant phone call, is quite sufficient.
- A security risk, as the more services that Hospify integrates with, the more vulnerable it is to hacking attacks and viruses. One of the main reasons that the 2017 WannaCry virus attack was so damaging to the NHS was that it was able to spread through poorly maintained integrations between digital services that had allowed security vulnerabilities to develop in their digital interfaces.

In the medium term, however, Hospify does intend to expose its internal APIs to properly authenticated third-party systems, so that data can be pushed into or pulled from Hospify, once correctly configured. This will enable a certain amount of integration with some EPR systems.

## Is Hospify GDPR compliant?

With regard to GDPR compliance, the architecture described in the answer to the previous question does comply with the GDPR.

Hospify does have ISO 27001:2017 accreditation (214722), does conform to the NHS Information Governance Toolkit (Org code: 8JN92), and is registered with the ICO (ZA239336), and work with a specialist consultancy, Securys who at as our Data Protection Officer and support us in our journey to be complaint with data privacy legislation all of which help ensure its compliance with UK health data protection regulation and the GDPR.

For more information on GDPR compliance, please see our Compliance White Paper, which can be downloaded from https://www.hospify.com/client-resources.

## Is Hospify HIPAA compliant?

Not at present. HIPAA (Health Insurance Portability and Accountability Act of 1996) is the United States' legislation that provides data privacy and security provisions for safeguarding medical information. Although HiPAA has many principles that are aligned to GDPR regarding the manner in data is handled and stored, it is a US federal standard that has no relevance or legal status in the UK or the EU. HIPAA has its own set of audit requirements, however, and there is no regulation over server hosting location. Hospify will be placed well to gain HIPAA compliance if a future regulatory change or product roadmap required it.

Hospify does hold a US SNAP-R license to export encryption technologies, which is important as we are selling technologies that use encryption via US app stores and platforms (Apple, Google) and therefore need to have this clearance.

## Can you blur elements in pictures?

No blur function is available as yet, but it's on the roadmap for 2020.

## Do you have to link messages to a particular patient?

You don't have to link to a patient, and this is in fact one of the reasons for our reluctance to integrate with EPRs. Because photos sent on Hospify are not directly linked to an individual patient, we're able to separate them entirely (i.e. put them on different servers) from the message data and sender metadata (which also have distinct and separated servers), and this adds considerably to the security of the data.

## As information is subject to retention guidelines, is there any way in which information can be set to automatically expire after a given period of time?

Yes. We have developed Hospify very much as an instant messaging (IM) tool. Its purpose is to replace non-compliant IM solutions such as WhatsApp and as such the conversations are of limited value over the long term. If something is pertinent to a patient's care, it should be recorded in the patient record just like the contents of a telephone conversation would be. To help with security and data retention we have therefore implemented an on-device data deletion function, which is set to 30 days. We have some plans to allow organisations to set alternative data deletion policies for its users via the Hospify Hub, but these have not yet been implemented.

## Are any protections in place against claims by users?

Hospify has full professional indemnity and cyber insurance, underwritten by Lloyds of London. A copy of our insurance policy is available on request.

## Is there anything a Trust or surgery has to do to comply when adopting Hospify?

To be fully compliant, health professionals and institutions that make the decision to switch over to Hospify need to tell their patients they're doing it. Don't worry - you don't have to tell them one by one. All you have to do is put a sentence or two in your privacy policy on your Trust's or practice's website. Something along these lines will suffice:

*"In order to protect patient confidentiality and abide with European health data protection guidelines, all staff in this Trust/medical practice use Hospify when they communicate using their mobile devices in the course of their work. Hospify securely encrypts messages, passes messages from handset to handset, holds no information from its users' communications on its servers, and keeps all communications within the European Economic Area, so abiding by UK data protection and the terms of the European General Data Protection Regulation. For more information please visit www.hospify.com."*

## Is there a practical limit on the number of messages stored?

No, other than the device's own storage capacity. Text messages take up little space and the 30-day deletion function, naturally caps message storage in the event that a user is communicating a lot of pictures.

## What are your arrangements for business continuity and disaster recovery? How is your data centre mirrored and if so, how far away is the mirror from the master site?

All our BR/DR policies are contained with our ISO27001 documentation and we are happy to share them on request. Our data centres are hosted on Amazon servers and mirrored within the EU. Our SLA with the company demands that mirroring occurs on at least three disparate locations. In addition, our phone-based architecture means data is effectively mirrored on device and is not reliant on a central server, further adding to Hospify's operational resilience.

## Does Hospify cross disciplinary and organisational boundaries? How do you verify users? Is there any facility for communicating with a patient?

Hospify is specifically designed to be cross-disciplinary and work across organisational boundaries. The service is also intended for use by patients. This is why the basic version is free for anyone to download and use in the Apple and Google app stores. Users have to grant other users' permission to chat to them, and that permission can be revoked, so a clinician can talk to a patient without handing over their phone number or email address and can then revoke the ability for that patient to contact them.