Process	Legal basis	Separate condition for storing and revealing sensitive data such as health data	Retention schedule
Storing data about our 'Supporters' and using it to send them our e-newsletter			
When people sign up to receive our information about our activities (primarily but not exclusively via our e-newsletter), we collect their names and contact details. For individual members, we also collect demographic data in order to monitor whether we are reaching a broad/representative cross-section of the local community.	Consent - For individual 'supporters', we have always explicitly phrased signing up as a supporter to mean consenting to receive our communications. A small number of people signed up as 'Healthwatch supporters' when they joined Community Southwark as organisational members. This did not include specific consent to receive the newsletter. However, because these are organisational representatives, communication with them is considered 'Business-to-Business' 'marketing' under our Public Task - Promoting and supporting the involvement of local people in the commissioning, the provision and scrutiny of local care services / Obtaining the views of local people regarding their needs for, and experiences of local care services and importantly to make these views known. However, we are reminding these recipients of our e-newsletter of their right to opt-out by unsubscribing.	For the demographic data collected from individual members: Explicit consent. (Submission of this data is not compulsory in order to receive the newsletter).	Supporters' details will be deleted when they request to unsubscribe from our newsletter or otherwise to be removed from our databases. If we receive returned mail or email from a person who does not have other contact details we will also delete their data from our Supporters database.
Storing and using non-anonymised data about attendance at our events			
When people sign up to attend our events we collect their names, contact details, and any access and dietary requirements in order to communicate about the event, record attendance, ensure fire safety, and support people at the event.	**Public Task -** Obtaining the views of local people regarding their needs for, and experiences of local care services and importantly to make these views known / Promoting and supporting the involvement of local people in the commissioning, the provision and scrutiny of local care services.	This may include disability and health information and implied ethnicity information based on language needs: **Consent**	Eventbrite data, planning sheets with personal data and sign-up sheets will be deleted after events (with only the number/type of attendees recorded)
Storing data about our volunteers and people who apply to volunteer with us			
We store information about - people who are currently volunteering with us, so that we can contact them, keep a note on their skills and interests, and monitor their demographic characteristics to ensure we are reaching a range of people from the local population. Emails between us and the volunteers may include sensitive information (e.g. to say they are unwell). Volunteers wishing to assist with our Enter and View visits will be required to undergo a Standard level DBS check. We do not record or store information on any convictions revealed by the DBS check, only on the date, reference number and overall outcome for those who became volunteers with us. Those applying to volunteer will be given further details about the data processing. - people who have previously volunteered with us, in case they request references and in order to record that we have fulfilled our legal obligations around DBS checks. - people who have applied to volunteer with us but who we decided were not a good match, in case they have queries about why this decision was made.	**Public Task -** Using volunteers helps us to carry out all of our tasks as the champion for patient and public voice in health and care services. As most of our volunteers are also local people, it also supports in itself our task of 'Promoting and supporting the involvement of local people in the commissioning, the provision and scrutiny of local care services. We collect data on our current and previous volunteers and applicants in order to run this function in a way which enables both efficiency and support for those who give up their time, thus making the best use of our public funds. DBS data (criminal records checks) This is not considered sensitive data in the same way , but in a category of its own. . The **legal basis** for requesting checks can be found here http://www.legislation.gov.uk/uksi/2012/3094/regulation/42/made.	Demographic data: **Consent** Sensitive information provided by the volunteer to us by email - This is provided proactively, indicating the volunteer's **consent** for us to receive it. If we need to *keep* the email or record the information somehow we will ask for the volunteer's **consent** to do so. DBS data (criminal records checks) This is not considered sensitive data in the same way , but in a category of its own. . The **legal basis** for requesting checks can be found here http://www.legislation.gov.uk/uksi/2012/3094/regulation/42/made.	Names and contact details of our volunteers and any other information needed to enable provision of a reference by us are destroyed around the end of the financial year including the 5-year anniversary of them stopping volunteering with us. Application forms and references: are destroyed around the end of the financial year following that in which someone applied but did not become a volunteer, says they no longer wish to volunteer with us, or stops responding to our communications. Demographic information is destroyed after monitoring and reporting is complete for the financial year following that in which someone says they no longer wish to volunteer with us, or stops responding to our communications. DBS checks: We will not keep any photocopy or other image of the certificate or its contents. However, if a person is accepted as a volunteer, we will indefinitely keep a record of: the person's name, date of issue of a certificate, type of certificate, reference number of
We store and where requested will publish minutes of our Advisory Group meetings, which include details on attendance, apologies, and contributions by our volunteer Advisory Group members.	**Public Task -** Advisory Grou p meeting minutes are kept and where necessary published in the interests of good governance so that we make the best use of our public funds.	We will not record sensitive personal data in Advisory Group minutes unless it is **manifestly made public** (e.g. if a member is well known to be part of an organisation or network of individuals sharing a protected characteristic).	We keep our Advisory Group minutes indefinitely as part of our governance arrangements
We may also store occasional emails and documents on a wide variety of work-related topics which contain information about the activities of our current and previous volunteers.	**Public Task -** general documents may be kept to support the whole range of our work	We will not record sensitive personal data in general documents unless it is **manifestly made public** (e.g. if a volunteer is well known to be part of an organisation or network of individuals sharing a protected characteristic).	*We are discussing a general document and email retention policy.*
Storing non-anonymised data about people's experiences and feedback about services			
Note that in very many cases, we store signposting information and feedback about services anonymously and many of the following will not apply.			
Storing non-anonymised feedback about services from our proactive engagement activities in our internal systems in order to ensure accurate analysis and reporting. This includes matching up and cleaning records (e.g. deleting duplicate responses), monitoring the demographic profile of participants, and contacting participants for clarification if needed. In cases where we have relied on Consent as our legal basis for publishing data which might *potentially* be identifiable to an individual (see below) we will store identifiable data to enable it to be matched to a person's consent and identity in case they choose to withdraw consent.	**Public Task** - Formulating views on the standard of provision and whether and how the local care services could and ought to be improved / Making reports and recommendations about how local care services could or ought to be improved/ Obtaining the views of local people regarding their needs for, and experiences of local care services and importantly to make these views known.	**Consent**	This data will be kept without anonymisation until both a) a 'clean' database of the data has been produced that can be anonymised without risks to accuracy and b) the report on the engagement project has been published. This is usually a period of a few months to a year. In cases where we have relied on Consent as our legal basis for *publishing* data which might potentially be identifiable to an individual (see below) we will store identifiable data as long as the report is in public circulation, in order to enable it to be matched to a person's consent and identity in case they choose to withdraw consent.
Storing non-anonymised information in our spreadsheet or in email systems about individuals' signposting queries, with their identity, to help us to: - Refer back to previous details of a case in order to better assist the person if they need further help. - Identify whether a person has contacted us several times on an issue, for balanced reporting of the number of times an issue has been raised with us - Identify how many separate individuals have contacted us, for monitoring purposes - Deal with potential complaints about our service.	**Public task** - Providing advice and information about access to local care services so choices can be made about local care services/Formulating views on the standard of provision and whether and how the local care services could and ought to be improved / Making reports and recommendations about how local care services could or ought to be improved Monitoring our activities and dealing with future complaints are also part of our public task in that we aim to make responsible use of public funds and provide a high-quality service.	**Consent.** *For email, by definition this has to be assumed by the fact that the person has sent us the email, but only for the duration it takes us to deal with the case.* In very rare cases if we had become aware that a person intended to take legal action against us about their case: **Legal claims**	This data will be kept until monitoring and reporting is complete for the financial year following that in which we received the query.
Keeping emails whereby we share information with providers, commissioners, the Local Authority or other outside agencies to resolve the specific problem which the individual has told us about, with that individual's consent, either to enable us to follow up on that case or to enable us to deal with potential complaints about our service.	While Consent is required for the action of sharing the information (see below), we store the email on the basis of our **Public task** - Providing advice and information about access to local care services so choices can be made about local care services. Monitoring our activities and dealing with future complaints are also part of our public task in that we aim to make responsible use of public funds and provide a high-quality service.	**Consent** is required to store any emails which included sensitive data, as with our spreadsheet. In very rare cases if we had become aware that a person intended to take legal action against us about their case: **Legal claims**	This data will be kept until monitoring and reporting is complete for the financial year following that in which we received the query.
Storing non-anonymised information in our internal systems about individuals' signposting queries and feedback about services, to help us in rare cases to: - Act on our legal obligations/duty to assist the Local Authority to carry out its own statutory functions with regard to safeguarding. - In very rare cases, pass on non-anonymised data or potentially identifiable data to a provider or commissioner of services in order to resolve very serious concerns. - Assist in the investigation of fraud or criminal activity, for the purposes of seeking legal advice or exercising or defending legal rights - Or as otherwise required by the law. We will also store the emails by which we share this information. Even when the data we share is not attached to a name or contact details, if there is any risk of future re-identification of the person, we may record the identity of the person in order to ensure we are fulfilling our data protection responsibilities.	**Vital interests (to prevent death or very serious harm)**	If using vital interests as the legal basis and the data includes sensitive data, the person must be **physically/legally unable to consent/refuse consent** (Healthwatch England describe it as not being 'reasonably possible' to get consent, such as in a life or death situation)	This data will be kept until the end of the financial year including the 5-year anniversary of us sharing the data in question.
	Legal obligations/assisting the Local Authority to carry out its own statutory functions with regard to safeguarding	**Sensitive data should not be revealed for legal and safeguarding purposes unless the law requires it.**	
	Public Task - Formulating views on the standard of provision and whether and how the local care services could and ought to be improved / Making reports and recommendations about how local care services could or ought to be improved.	**Public interest in the area of public health**, such as… ensuring high standards of quality and safety of health care. This may occasionally apply to temporarily *storing* sensitive data even when we might not ultimately need to *share* it.	
	Consent should not be requested in the rare cases where we suspect we might have to override refusal of consent in the fulfilment of our Public Task or safeguarding functions - we must simply inform the patient of our actions and of their right to object. In some less serious cases where our Public Task does not require that we share non-anonymised data, we might request consent from the patient to do so and to store the related data.	**Consent** should not be requested in the rare cases where we suspect we might have to override refusal of consent in the public interest or for safeguarding purposes - we must simply inform the patient of our actions and of their right to object. In some less serious cases where Public Interest does not require that we share non-anonymised sensitive data, we might request consent from the patient to do so and to store the related data.	
Sharing non-anonymised data about people's experiences and feedback about services			
Note that in very many cases, we share signposting information and feedback about services anonymously and many of the following will not apply. We never publish non-anonymised data in our public reports.			
Sharing information with providers, commissioners, the Local Authority or other outside agencies to resolve the specific problem which the individual has told us about, for that individual.	**Consent**	**Explicit consent**	
	Vital interests (to prevent death or very serious harm)	If using vital interests as the legal basis and the data includes sensitive data, the person must be **physically/legally unable to consent/refuse consent** (Healthwatch England describe it as not being 'reasonably possible' to get consent, such as in a life or death situation)	
	Legal obligations/assisting the Local Authority to carry out its own statutory functions with regard to safeguarding	**Sensitive data should not be revealed for safeguarding purposes unless the law requires it.**	
Sharing information with commissioners/providers about how services must improve, and information about a specific case needs to be explained in order to enable this or very occastionally where the person's identity must be revealed in order to resolve very serious concerns. This is very rare. Example: A Serious Incident (legally defined) has been reported by the patient, but was not known by the hospital. The hospital might need the patient's identity in order to do a root cause analysis and prevent this from happening again.	**Public task** - Formulating views on the standard of provision and whether and how the local care services could and ought to be improved / Making reports and recommendations about how local care services could or ought to be improved.	If no further *sensitive* data will be revealed to the provider than that which is already known to them – e.g. if all they will find out is that the person has raised their concern with HWS or details of what went wrong in their care rather than their actual health status, : **no separate condition is required.** If there is a risk that further sensitive data might be revealed to the provider than that which is already known to them (and it is rare that this would be necessary): **Public interest** in the area of public health, such as… ensuring high standards of quality and safety of health care.	See details in the section above for information about the storage and retention schedule for information shared via the processes described here.
	Consent should not be requested in the rare cases where we suspect we might have to override refusal of consent in the fulfilment of our Public Task - we must simply inform the patient of our actions and of their right to object. In some less serious cases where our Public Task does not require that we share non-anonymised data, we might request consent from the patient to do so.	**Consent** should not be requested in the rare cases where we suspect we might have to override refusal of consent in the public interest - we must simply inform the patient of our actions and of their right to object. In some less serious cases where Public Interest does not require that we share non-anonymised sensitive data, we might request consent from the patient to do so.	
Sharing information with the public via our general quality reports and thematic reports. It is less likely that patients described in this way would be identified, but more likely that if they were identified this would reveal information not already known.	In the vast majority of cases we will take great care to ensure that people are not identifiable from the data we published in our reports, even if we do not publish obvious identifying details. We could include direct quotes and personal stories, but for example mixing up details from differrent patients. However, there may be some examples where patients take the time to share their invididual story with us and are keen that it be published in its complete state. We will make sure to discuss this with people and ensure enthusiastic **consent,** so as to reduce the risk of needing to erase published data if the individual withdraws consent at a later data.		