Customer Data Request Form (Metadata Only)

Please read the instructions carefully and include as much detail as possible so our team can best assist you. This form is used to request **metadata**. This may include:

1. Date and timestamps of Hypercare messages delivered and read by Users,
2. Contents and timestamps of SMS sent via Hypercare and
3. Contents and timestamps of Pages sent to physical pagers via Hypercare.

Note, contents of SMS and Pages sent to physical pages via Hypercare are only available for 30 days from the time it was sent. This form needs sign-off from **at least one** authorized person of the organization that has been indicated as an Administrator of Hypercare. Do not include private health information (PHI) in any of the fields. The request should be as narrow as possible in order to fulfill your needs. For more information, please refer to the Customer Data Request Policy.

Please email the signed form to support@hypercare.com for processing. Requests take at least 2 business days to process.

Reason for request

(e.g. critical incident debrief, patient complaint, quality assurance activities).

Affected users

Full name of affected user(s) and email(s) associated to their Hypercare account.

Date and time range of metadata being requested

Type of metadata being requested

Select all that apply.

- ☐ Metadata of Hypercare messages **only** exchanged between Affected Users
- ☐ Metadata of **any** Hypercare messages to or from the Affected User(s)
- ☐ Metadata of SMS sent via Hypercare to Affected User(s). Metadata requested:
  - ☐ Date and timestamp
  - ☐ Contents of SMS
- ☐ Metadata of Physical Page sent via Hypercare to Affected User(s). Metadata requested:
  - ☐ Date and timestamp
  - ☐ Contents of Physical Page

HYPERCARE

Other details of the request

Name(s) and email address(es) the requested metadata should be sent to

Will you inform the affected user(s) that their data has been accessed?

Yes ▢ **No** ▢

We, the undersigned, have the authority to make this data request and to handle any Personally identifiable information (PII) therein on behalf of our organization. We attest that this request is for legitimate clinical, business, privacy, or security purposes, and that all other avenues to obtain the information (e.g. requesting it from the user(s) directly) are not available or feasible. We will comply with any applicable privacy and security laws within our jurisdiction with respect to handling personal data and personal/private health information.

Administrator Signatory

_____
Signature

_____
Name

_____
Title

_____
Organization

_____
Date

Optional: Secondary Administrator Signatory

_____
Signature

_____
Name

_____
Title

_____
Organization

_____
Date