

Health and
Social Care

Data Protection Impact Assessment (DPIA) template

The DPIA outlines

- what personal data will be processed?
- what will the information be used for?
- any risks associated with the processing.
- steps taken to mitigate against the risks.

Project/System name:
encompass (Electronic Health and Care Record (EHCR) ecosystem, sharing Patient Identifiable Information (PII) between health and care staff across NI)
Service or Project Lead – completing the DPIA
Name: [REDACTED] Senior Programme Manager Telephone: [REDACTED] Email Address: [REDACTED]@hscni.net
Department/Location (include full address)
Business Services Organisation 2 Franklin St Belfast BT2 8DQ
Directorate:
Business Services Organisation encompass on behalf of HSCNI
Date DPIA commenced:
6 January 2020

STEP 1. DESCRIBE THE PROCESS

Briefly describe below the purpose of the data processing and what the project aims and objectives are?

Please **do not** embed documents or hyperlinks. Instead, attach relevant documents as appendices and clearly indicate which section of the appendices provides the necessary info in relation to each question below.

- **what information will be collected,**
- **how it will be collected,**
- **how it will be used / processed**
- **where it will be stored**
- **who will have access to it (including any 3rd parties)**
- **the arrangements for and when it will be deleted**

As part of this first stage, the service area may need to complete a Data Flow Map. This can be a diagram but should accurately describe the stages of the data flow from beginning to end.

encompass is a major enabling programme to underpin the much-needed transformation of HSC services and will replace multiple aging Trust systems and numerous paper records and manual workflows. encompass will deliver an integrated Health and Care Record with significant core functionality across the acute, community and primary care Out of Hours sectors. Incorporating international interoperability standards [REDACTED]

Functionality to deliver advancements in patient safety and experience are a core part of implementation [REDACTED]

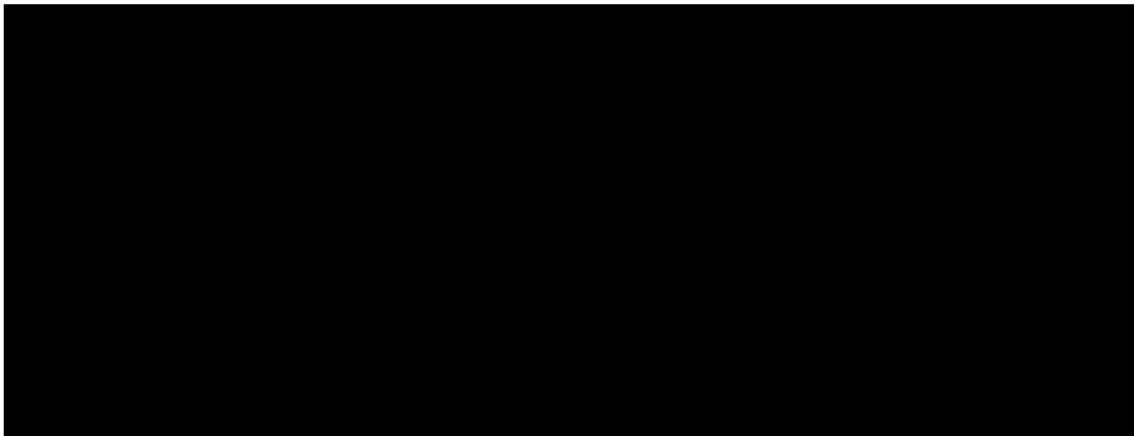
The development of this single patient record holding a wider range of information has the potential to improve the accuracy and quality of the care delivered to our citizens. This will be balanced against the need to ensure that patient and client confidentiality is maintained and that the information is only used for its intended purpose.

Following a competitive dialogue procurement and full business case approval process from 2018 to 2020, the contract for the integrated health and care record solution was awarded to Epic in May 2020. Epic are global leaders in this technology and also in their structured implementation approach, tools and quality of support to help ensure success.

The primary aim of the encompass programme, built on Epic's Electronic Health and Care record enterprise application (EHCR), is to ensure all NI citizens benefit from a shared EHCR, and all practitioners in NI can access this information where and when it is needed to deliver safe and effective health and care.

1. What information will be collected?

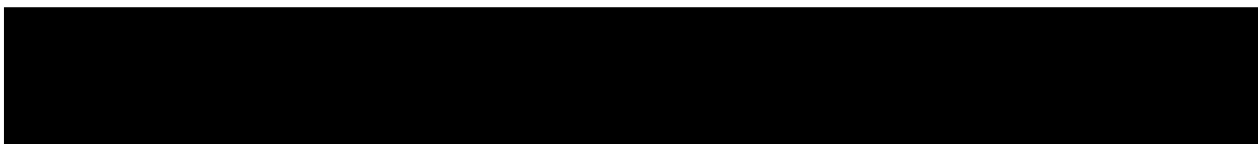
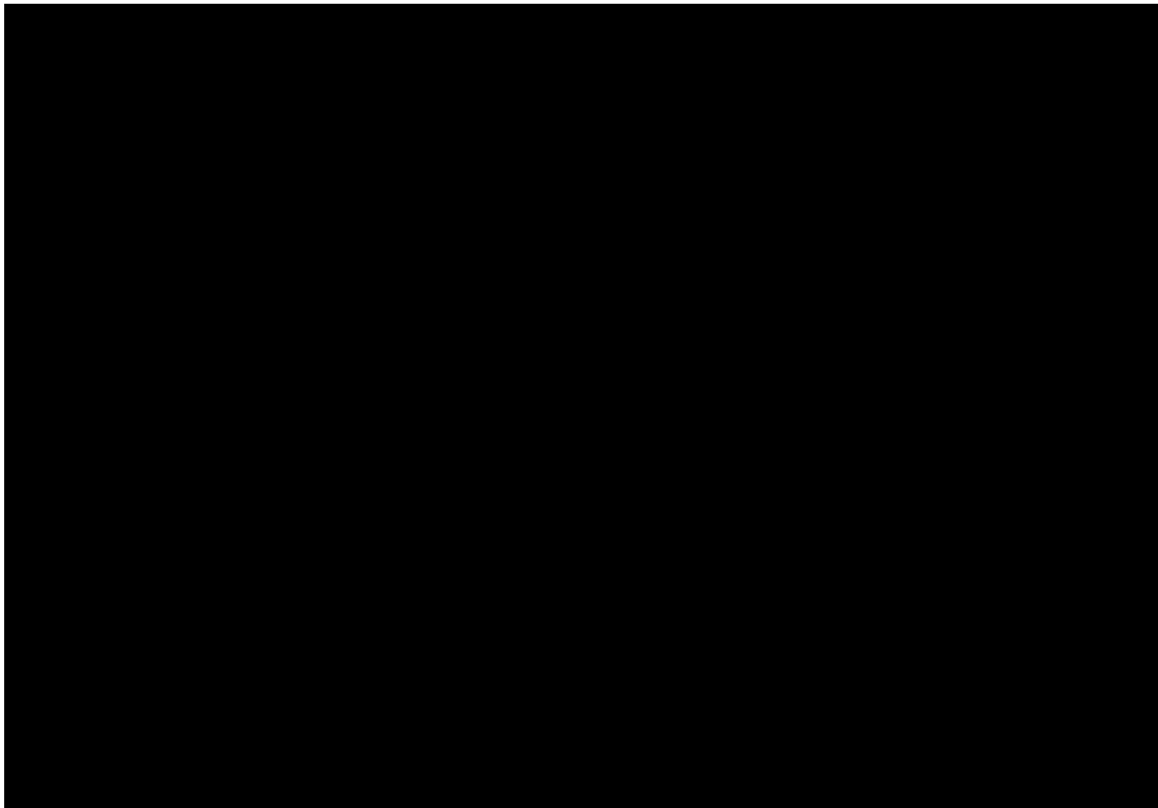
The encompass capabilities will collect a comprehensive range of health and social care data, including:



Much of this information will have been collected previously (and managed in legacy systems and paper records).

2. How will it be collected?

Data will be collected through a range of methods:



3. How will it be used/processed?

[Redacted]

The collected data will be used and processed for multiple purposes currently:

- **Direct Care:** To provide safe, high-quality, and effective care across all HSCNI facilities. This includes real-time access to patient / service user records for healthcare professionals [REDACTED]
 [REDACTED]
 [REDACTED]
 [REDACTED]
 [REDACTED]
- **Staff and Affiliate staff data:** To facilitate training, identification of super-users and provisioning will inform Role Based Access Control (RBAC) and legitimate relationships to access records. [REDACTED]
 [REDACTED]
 [REDACTED]
 [REDACTED]
 [REDACTED]
 [REDACTED]
 [REDACTED]
 [REDACTED]
- **Reporting:**
- For operational reporting [REDACTED]
 [REDACTED] and for statutory, regulatory and performance reporting returns [REDACTED]
 [REDACTED] reporting capabilities are accessible to select users only via RBAC.
- For Compliance: to ensure compliance with statutory obligations e.g. to ensure safe, high-quality, and effective care across HSCNI.

Notwithstanding the above, for the purposes of clarity, the use of the encompass system is for direct care and the data extracted from encompass is being used for reporting purposes. Note that personal data is collected for "specified, explicit and legitimate purpose, and not processed further in a manner incompatible with those purposes".

- **Support Arrangements:** to support authorised users (ahead of go live, and throughout ongoing operation)
 - [REDACTED]
 - [REDACTED]
[REDACTED]
 - [REDACTED]
[REDACTED]
[REDACTED]
 - [REDACTED]
 - [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]

- **Research:** Currently no data is being processed to support research trials³.

4. Where will it be stored?

Data is stored [REDACTED]
[REDACTED]
[REDACTED] compliant with relevant data protection regulations.

Architecture and Security for encompass

[REDACTED]
[REDACTED]

[REDACTED]

³ [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

- [REDACTED]
[REDACTED]ation will access. At the heart of Epic's architecture is the operation
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

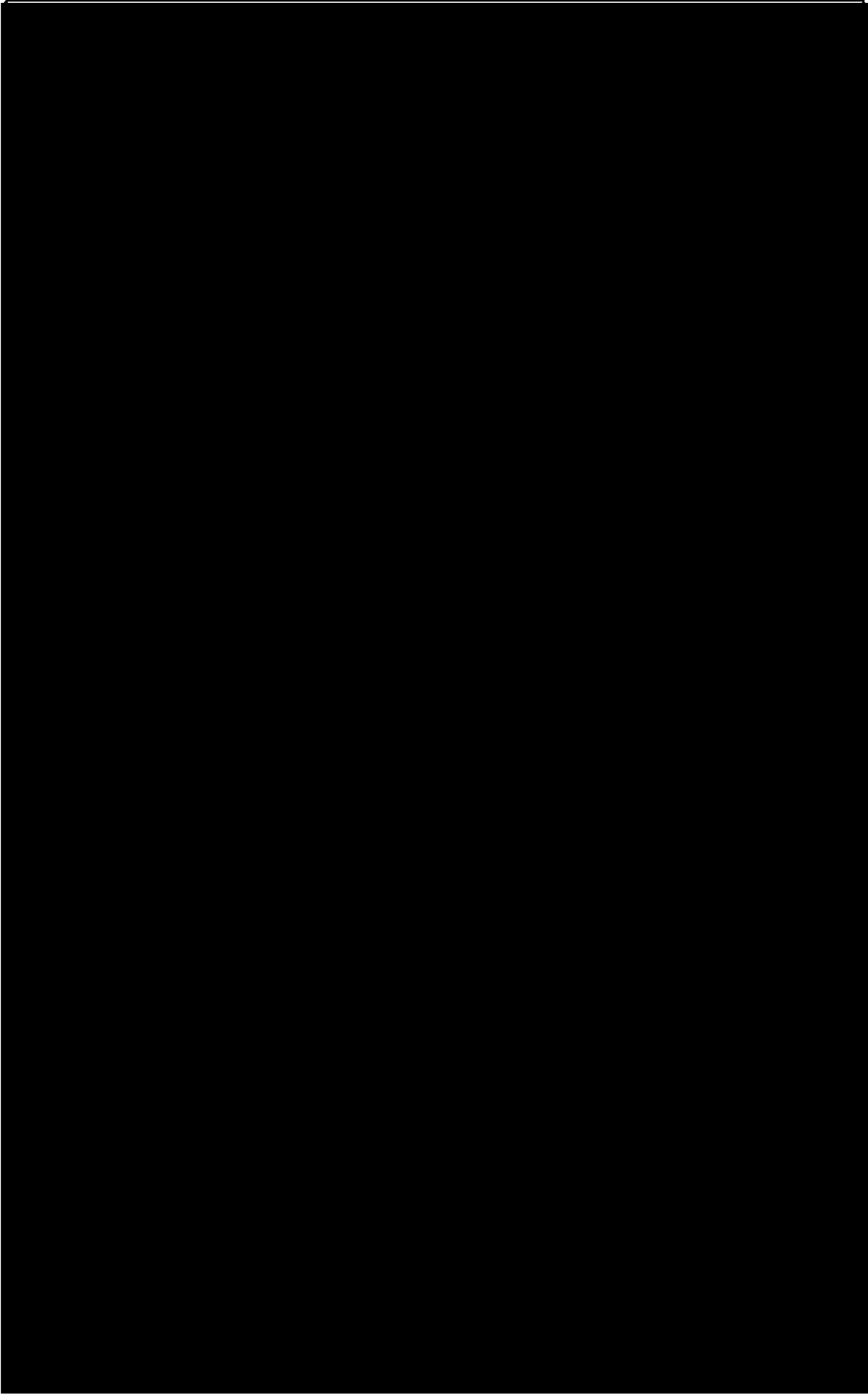
[REDACTED]

[REDACTED]

5. Who will have access to it (including any 3rd parties)?

The system uses RBAC to ensure that only authorised users can access certain records, features, and data items.

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]



[REDACTED]

[REDACTED]

[REDACTED]

6. The arrangements for and when it will be deleted?

Data retention and ensuring records are 'Put beyond Use' will follow established policies and legal requirements, including those governed and controlled by Good Management Good Records (GMGR) (please refer to that document for more detail).

[REDACTED]

If your processing includes the use of emerging technologies e.g. **Artificial Intelligence (AI)** then this needs to be specified in more detail below:

Please see the ICO's guidance on AI [AI and data protection risk toolkit](#) | ICO

Please see BSO's policy on AI (attached at Appendix D)

Clinical decision support within encompass will use personal information to support health and care professional decision makin [REDACTED]

[REDACTED]

As the human involvement in the decision-making process has not been removed the clinical decision support within the encompass solution does not constitute solely automated decision making as defined by Article 22 UK GDPR.

[REDACTED]

[REDACTED]

STEP 2. ASSESS THE NEED FOR A DPIA

Screening Questions - The following are intended to help decide whether a full DPIA is necessary.

Number	Question	YES	NO	Either way please provide further details here
1.	Does the [encompass] project involve collecting new/additional personal information about individuals?	☒	☐	
2.	Does the [encompass] project involve gathering information in a new way?	☒	☐	
3.	Does the [encompass] project establish a new way of identifying individuals?	☐	☒	
4.	Will the [encompass] project use an individual's personal data already held in an existing system (manual or electronic) for a new purpose or in a new way?	☒	☐	
5.	Will the [encompass] project disclose or share personal information with organisations or people/staff who have not previously had routine access to it.	☒	☐	
6.	Will the [encompass] project involve matching or linking with personal information held by a different organisation(s) or departments or in different datasets e.g. combining, comparing or matching personal data obtained from multiple sources	☒	☐	
7.	Will the [encompass] project change the way personal information is managed, stored or secured (e.g. new	☒	☐	

	database, new location, cloud storage)			
8.	Is this a system or process that has not had a DPIA completed previously? Or is there a DPIA in place but this is a new instance of processing?	New ☐ Update ☒ <i>If this is an update to an existing DPIA please provide details</i> <i>Converted to current standard template.</i> <i>Updated in line with current landscape and recommendations from ICO and Information Governance Advisory Council.</i> <i>Updated in line with new My Care DPIA</i>		

If you have answered **YES** to any of the above, **continue to Step 3** and complete the DPIA.

If you have answered **NO** to all of the 8 questions above **please proceed to Step 12** and record the outcome.

STEP 3. DESCRIBE THE PERSONAL DATA BEING COLLECTED

What Personal data is being collected? This applies to any stage of the process (tick only those that apply). *this list is not exhaustive

Personal Data required	Tick all that apply	Provide details of who the personal data relates to: i.e. Service User/staff/relative/Other (please detail)
------------------------	---------------------	--

Please provide justification for the personal data being processed e.g. Do you need full postcode or would partial postcode be sufficient? Do you need full Date of Birth or would age be sufficient?

These data items are required to enable the delivery of health and care services to the individuals [REDACTED]. In addition, elements of demographics are used to ensure safe matching of historic or external data against individuals. Physical descriptions may be included in care notes or correspondence where relevant to the provision of medical or social care services.

Special Category data (sensitive personal data)	Tick all that apply	Provide details of who the Special Category data relates to: i.e. Service User/staff/relative/Other (please detail)
---	---------------------	---

STEP 4. LAWFUL BASIS FOR PROCESSING
What is your UK GDPR Lawful Basis for processing/sharing personal data? See Appendix 2 for further information or seek IG advice.

Article	Lawful basis	Tick
6 1 (a)	Consent	
6 1 (b)	Contract	☒
6 1 (c)	Legal obligation (Please detail which legislation* this will come under)	☒
6 1 (d)	Vital Interests	☒
6 1 (e)	Public Task (please detail sections of the legislation which support Public task legal basis below)	☒
6 1 (f)	Legitimate Interests	☐

Please provide details of the relevant sections of legislation in addition to UKGDPR, which support your legal basis

Health and Social Care (Reform) Act (Northern Ireland) 2009

Section 21: It is the duty of an HSC trust to exercise its functions with the aim of improving the health and social well-being of, and reducing health inequalities between, those for whom it provides, or may provide, health and social care.

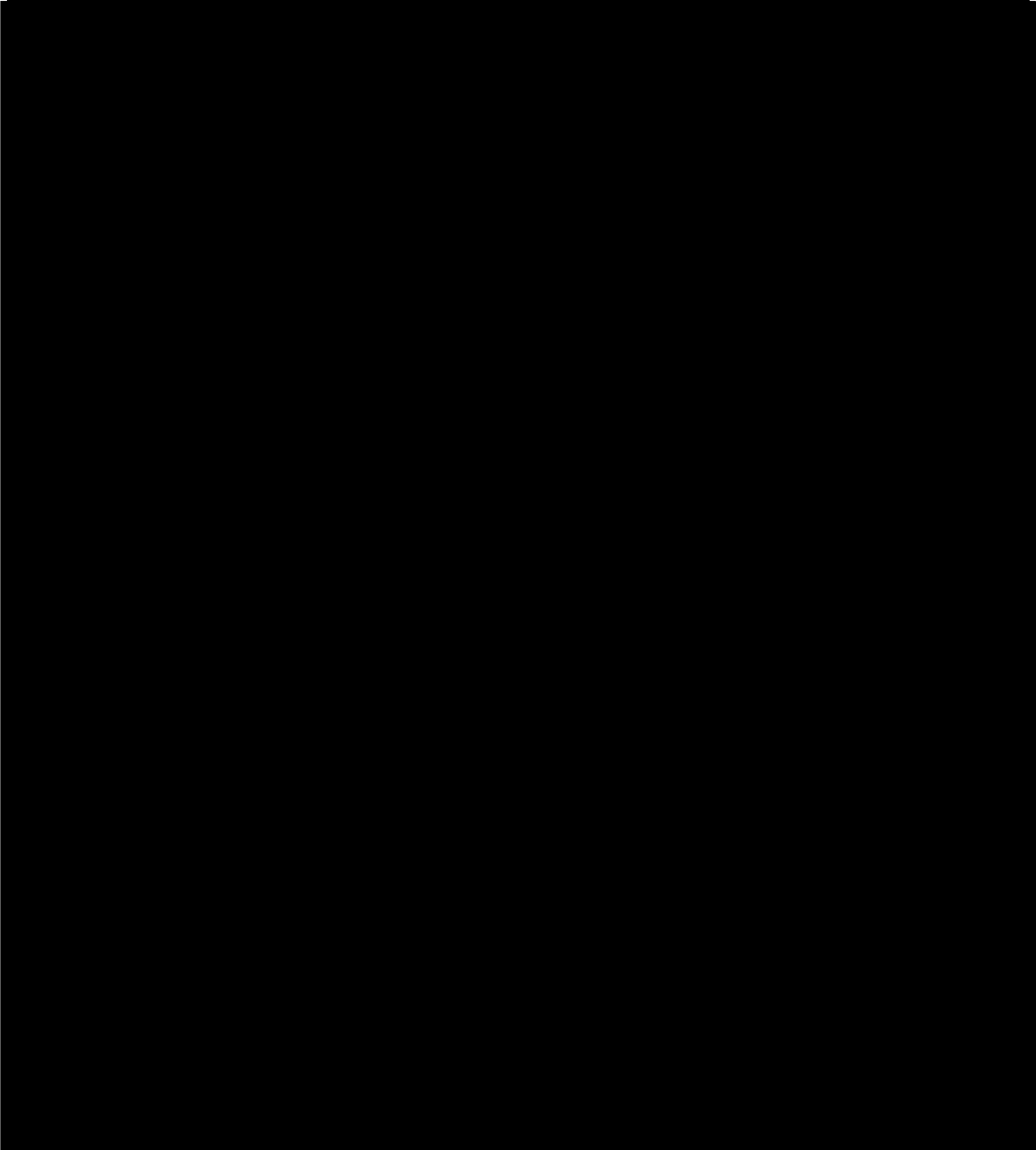
Specific examples of when each of the identified lawful basis may apply can be referenced in Appendix 3.

If applicable what is your UK GDPR Lawful Basis for processing/sharing **special category data**? See Appendix 2 for further information or seek IG advice.

Article	Lawful Basis	Tick
9 2 (a)	Consent	☐
9 2 (b)	Employment social security social protection law	☐
9 2 (c)	Vital Interests	☒
9 2 (d)	Legitimate interest	☐
9 2 (e)	Already public	☐
9 2 (f)	Establishment, exercise or defence of Legal claims or judicial capacity	☐
9 2 (g)	Public Interest	☒
9 2 (h)	Health and Social Care treatment or management of HSC systems	☒
9 2 (i)	Public Interest in the area of Public Health, Quality and Safety of Health Care	☒
9 2 (j)	Archiving in the public interest, scientific, historical research or statistical purpose	☐

STEP 5: ASSESS SECURITY OF THE INFORMATION

Will the information be shared with, hosted by or transferred to another organisation or third party?



Data Controllers

Health and Social Care Trusts are individual data controllers. BSO acts as the Data Processor on behalf of the Trusts and Affiliate (partner HSCNI, regulators and non HSCNI healthcare providers) organisations in accordance with the HSCNI Data Controller and Data Processing Memorandum of Understanding (MoU) issued under Article 28(3) of UK GDPR, August 2019 and updated November 2021; the list of all 3rd party sub-processors are below.

Data Processors

BSO, as Data Processor [REDACTED]

[REDACTED]

In addition to the data processors listed in above [REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

Sub-Processors

[REDACTED]

[Redacted]

Where 3rd party suppliers are engaged, appropriate information security management, confidentiality and data protection obligations are included within the contract in relation to UK laws including Data Protection Act 2018 and UK GDPR. These clauses will be kept under review to ensure that they remain compliant with any changes resulting from amendments to UK GDPR or Data Protection Legislation. [Redacted]

[Redacted]

Affiliates will act as a sub-processors and act under the instructions of the processor (BSO). Where affiliates are engaged, they must comply with all appropriate information security management, confidentiality and data protection obligations in relation to UK laws including Data Protection Act 2018 and UK GDPR.

[Redacted]

How will you secure the information in Transit? Tick which apply

[Redacted]	

[REDACTED]	[REDACTED]
------------	------------

[REDACTED]

ICT Input			
-----------	--	--	--

[REDACTED]

You should consider the impact of the new process or system will have on all your stakeholders. Who have you consulted with?

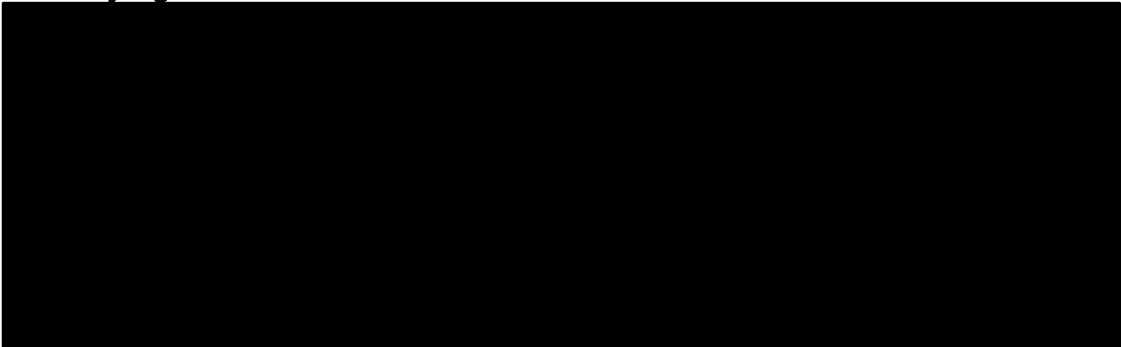
This ongoing engagement strategy is designed to consider the impact of the new system on all involved parties and will continue throughout the lifecycle of encompass.

1. Service Users:

- [illegible]



6. Statutory Agencies:



Other Consultations:



Public Awareness and Education:

To support public awareness and education, encompass has a website and a communications plan where the Privacy Notices and FAQs have been posted. For more information see [Appendix D – Supporting Documents \(Comms\)](#)

If you have not consulted with affected staff or service users please explain your reason for this below:

N/A

STEP 8. EVALUATE THE PROCESS		
Function creep is the gradual widening of the use of a technology or system beyond the purpose <u>for which it was originally intended</u> as set out this DPIA, especially when this leads to potential invasion of privacy. Are you content with the measure in place that there is no risk of function creep? If No, please ensure the risk of function creep is included at Step 11	YES ☒	NO ☐
Future developments and envisaged future use of data It is envisaged that in the future the system will develop and offer new capabilities and data processing [REDACTED]		

This means that there is the potential that some of the health and social care data comprised within encompass will be used for different purposes in the future. If encompass decide to pursue any additions or improvements which result in new uses of data characteristics that are not considered in this current DPIA, these future developments will be assessed and reviewed to help identify and minimise the data protection risks and to ensure any future use of the health and social care data comprised in encompass complies with data protection principles.

The development of the system at this stage will require amendments to this DPIA, or the drafting of a separate DPIA, depending on how fundamental the changes are in the purposes for which encompass data is processed. This will also involve careful assessment of the lawful basis section and whether the new purposes fall within the lawful bases already being relied upon, or whether they fall within a different lawful basis, as well as how they interact with the common law duty of confidentiality.

The responsibility for monitoring relevant updates to any "live" information governance documentation, including this DPIA, rests with the encompass Information Governance Advisory Council in conjunction with the data controllers (each data controller is represented on IGAC) and encompass input. If there are any future iterations or developments to the system this will be reviewed to ensure that it will comply with data protection legislation

What measures will be in place to ensure the accuracy and quality of the data being processed?

To ensure the accuracy and quality of the data being processed within encompass, multiple measures are in place and some are developing:

1. Initial Data Accuracy and Quality Assurance:

- The accuracy and quality of the initial health and care records are assured through defined processes [REDACTED]
- HCN matching and DQ process [REDACTED]
- Each Trust adheres to its Record Keeping / Management Policy to maintain ongoing accuracy and integrity of the data once migrated into encompass.

2. User Input and Validation:

- Patients, service users, or proxies (Users) can view, validate / feedback and input data into their health and care records digitally.
- This user-generated data is subject to review and processing by Health and Social Care (HSC) staff through encompass.
- User inputs cover a vast arrange and range of use cases during healthcare delivery.
- It is recognised that there will be some inaccurate or incomplete information in some records, however enabling this information to be updated by the patient or proxy themselves will improve the quality of record keeping
- Array of workflow and data validation rules [REDACTED]
- Data Quality team implemented SOP [REDACTED]

3. Monitoring and Auditing Data Interactions:

- Additional data gathered using encompass, such as access and audit logs, are systematically gathered, monitored, and reviewed as required
- Encompass provides robust mechanisms for logging and auditing [REDACTED]
- [REDACTED] to maintain data integrity and respond to any discrepancies or unauthorised access promptly
- [REDACTED]

What measures will be in place to ensure the data minimisation principle is adhered to?
i.e. only processing or sharing what is necessary and the minimum amount needed for the purpose.

To ensure adherence to the data minimisation principle, targeted measures are in place and some are emerging. These measures are designed to ensure that only the necessary and minimum amount of data needed for specific purposes is processed or shared. Here are the key strategies:

1. Role-Based Access Control (RBAC):

[REDACTED]

2. Purpose Limitation Protocols:

[REDACTED]

3. Data Segmentation and Restriction:

[REDACTED]

4. Proactive Audits and Compliance Checks:

[REDACTED]

5. Privacy by Design:

[REDACTED]

6. Clear Roadmap and Stage Plans:

[REDACTED]

7. Training and Awareness:

[REDACTED]

8. Feedback Mechanisms:[REDACTED]**9. Review and Update Policies and Governance (Decision Rights) Models:**[REDACTED]**STEP 9. CONSIDERATION OF DATA SUBJECTS RIGHTS****1. Right to be informed**

Is the [encompass] project covered by an existing privacy notice?
(If no, a bespoke privacy notice will be required and approval sought through IG Department)

YES
☒

NO ☐

Yes – Published – encompass Site (encompass Privacy Notice and encompass My Care Privacy Notice)

2. Right of access

The organisation is obliged to provide personal information upon request in line with Data Protection Act 2018 and UK GDPR.
Have you considered how this will be achieved in your project?
Please provide details below:

YES
☒

NO ☐

Access to any part of a health and care record that is not accessible to a patient or service user through My Care, can be requested from the relevant Health and Social Care Trust in accordance with the Subject Access Request procedure under the Data Protection Act 2018.

STEP 10. PERSONAL INFORMATION SHARING AGREEMENTS

Is there or will there be a **contract** in place containing specific data protection clauses* with the organisation(s) you plan to share information with?

YES
☒

NO ☐

** the contract clauses will need to reflect the mitigations identified at Step11 to minimise the data protection risks*

If **NO**, in the absence of a contract what agreement will be in place?
e.g. Data Sharing Agreement, Data Access Agreement, Memorandum of Understanding
Please provide details below:

All HSC organisations using encompass have in place:

- Direct Care MOU (2022)
- Records Management Policy
- Data Protection Policy

All 3rd party Technical and Infrastructure service providers [REDACTED]
have contracts in place in line with data protection and privacy elements. All pertinent mitigations in step 11 have been passed on to the appropriate contract owner and are being cross referenced against the contracts to establish if there are any areas of risk.

Step 11. IDENTIFY, ASSESS AND MITIGATE ANY DATA PROTECTION RISKS

In this section you are asked to first identify and describe the specific risks associated with this project/process and assess the nature of potential impact on individuals. You will then describe the measures you could take to reduce each identified risk.

To assist you in identifying potential or likely privacy risks you will find a non-exhaustive list of possible risks at Appendix 3.

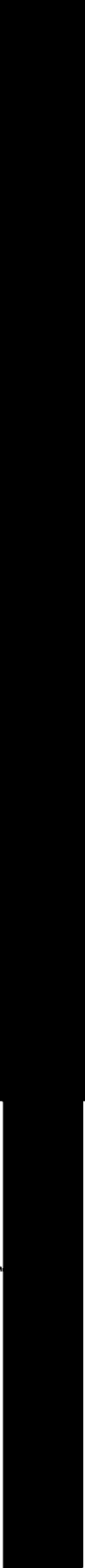
The HSC Regional Risk Matrix and Regional Impact Table below will also help you to assess the level of risk.

Likelihood Scoring Descriptors	Impact (Consequence) Levels				
	Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Catastrophic (5)
Almost Certain (5)	Medium	Medium	High		
Likely (4)	Low	Medium	Medium	High	
Possible (3)	Low	Low	Medium	High	
Unlikely (2)	Low	Low	Medium	High	High
Rare (1)	Low	Low	Medium	High	High

There are 7 overarching risks to the data subject(s), which have a range of causes and impacts, further outlined in the tables below:

1. The user accesses and / or shares a record they shouldn't
2. The user sees and / or shares information they shouldn't
3. The information that the user sees and / or acts on is incorrect or incomplete
4. The information viewed is harmful to the viewer or the subject
5. The information viewed isn't understandable or is misunderstood
6. Information security (to one or many) is compromised
7. Public confidence reduces

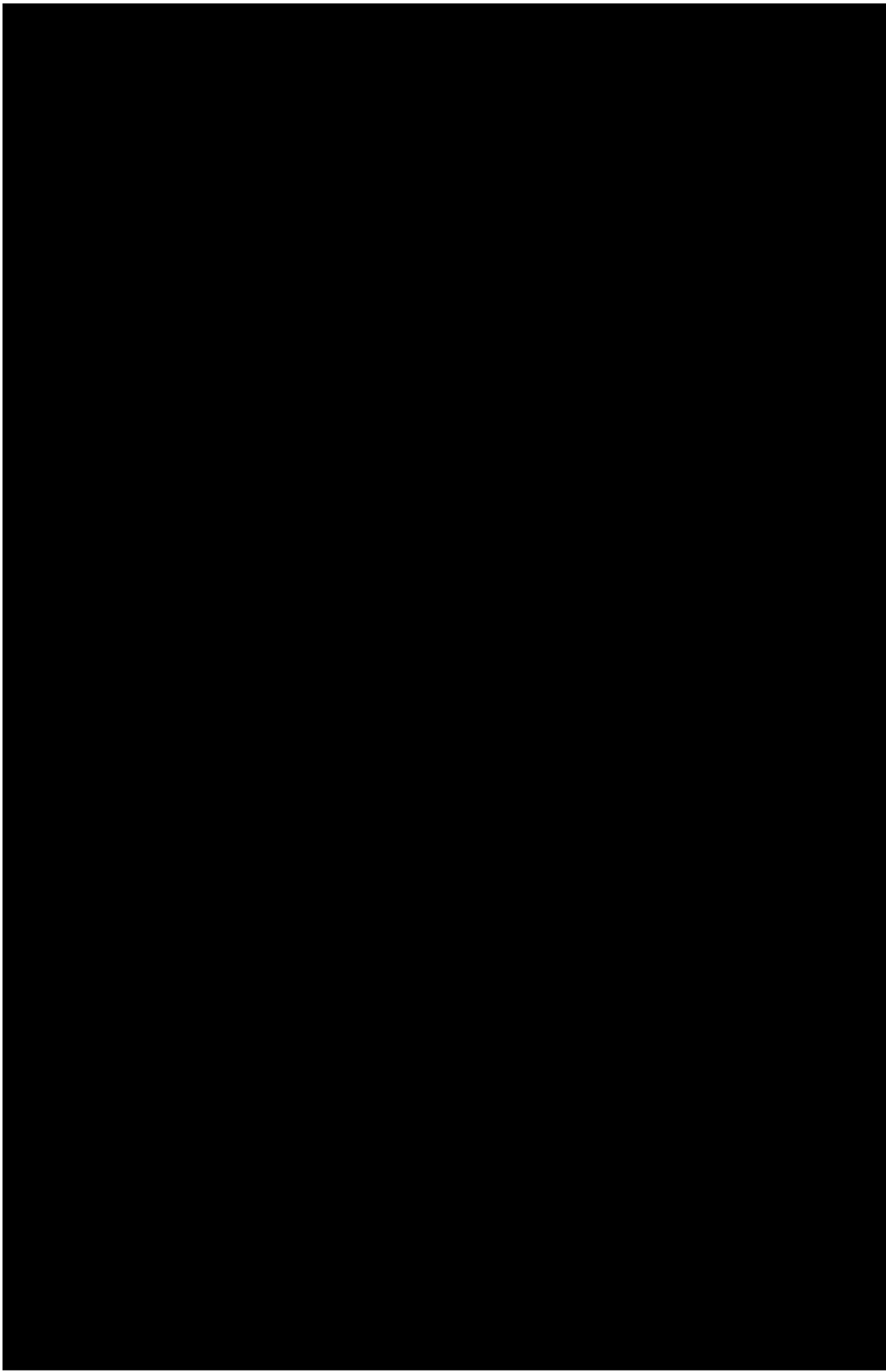
Whilst it is significantly more likely for human error, given the scale and sensitivity of the data processed, the threat surface, and the increasing threats from the wider geo-political environment, the approach to information governance and security needs to be consistent and involve systemic focus.

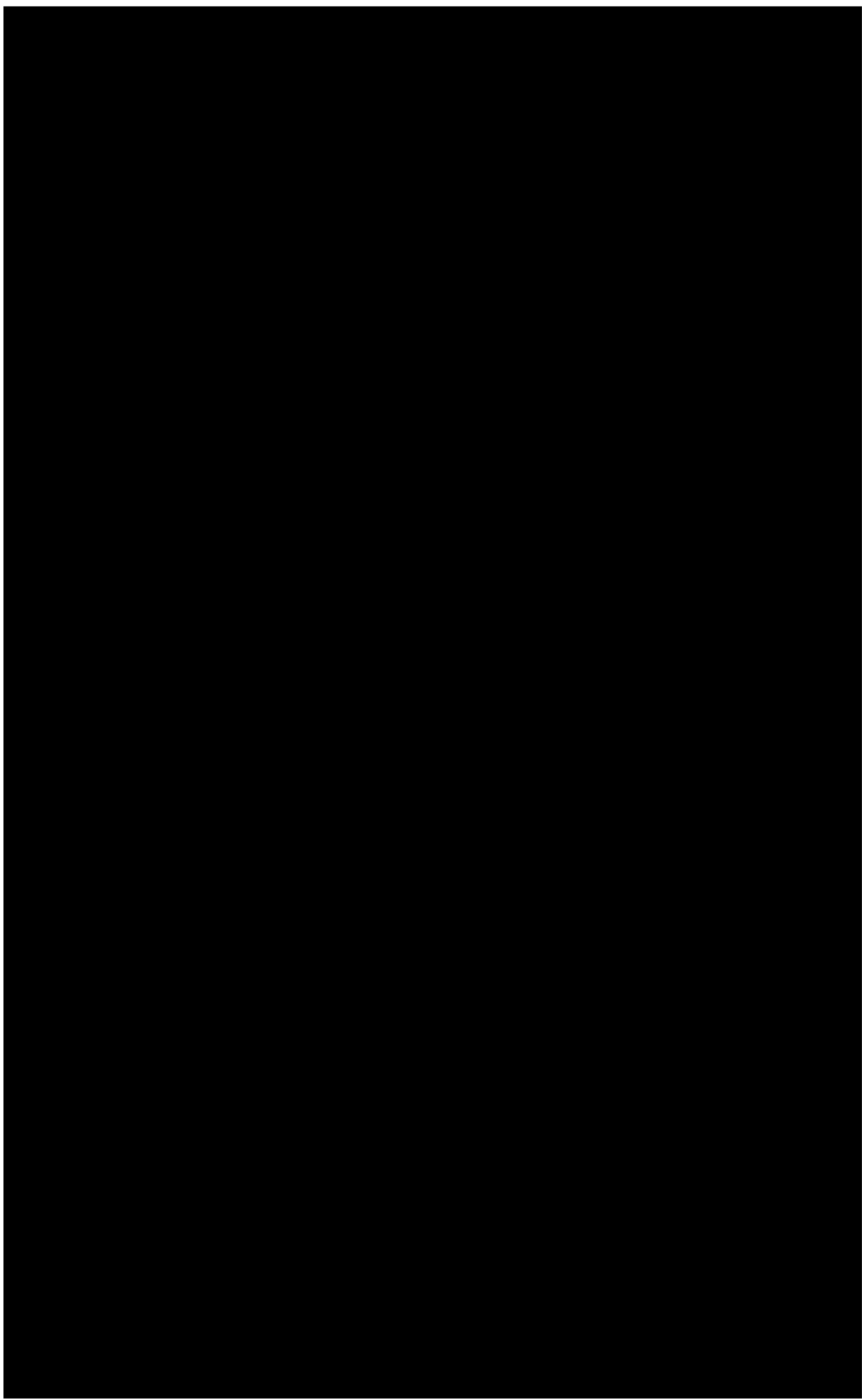


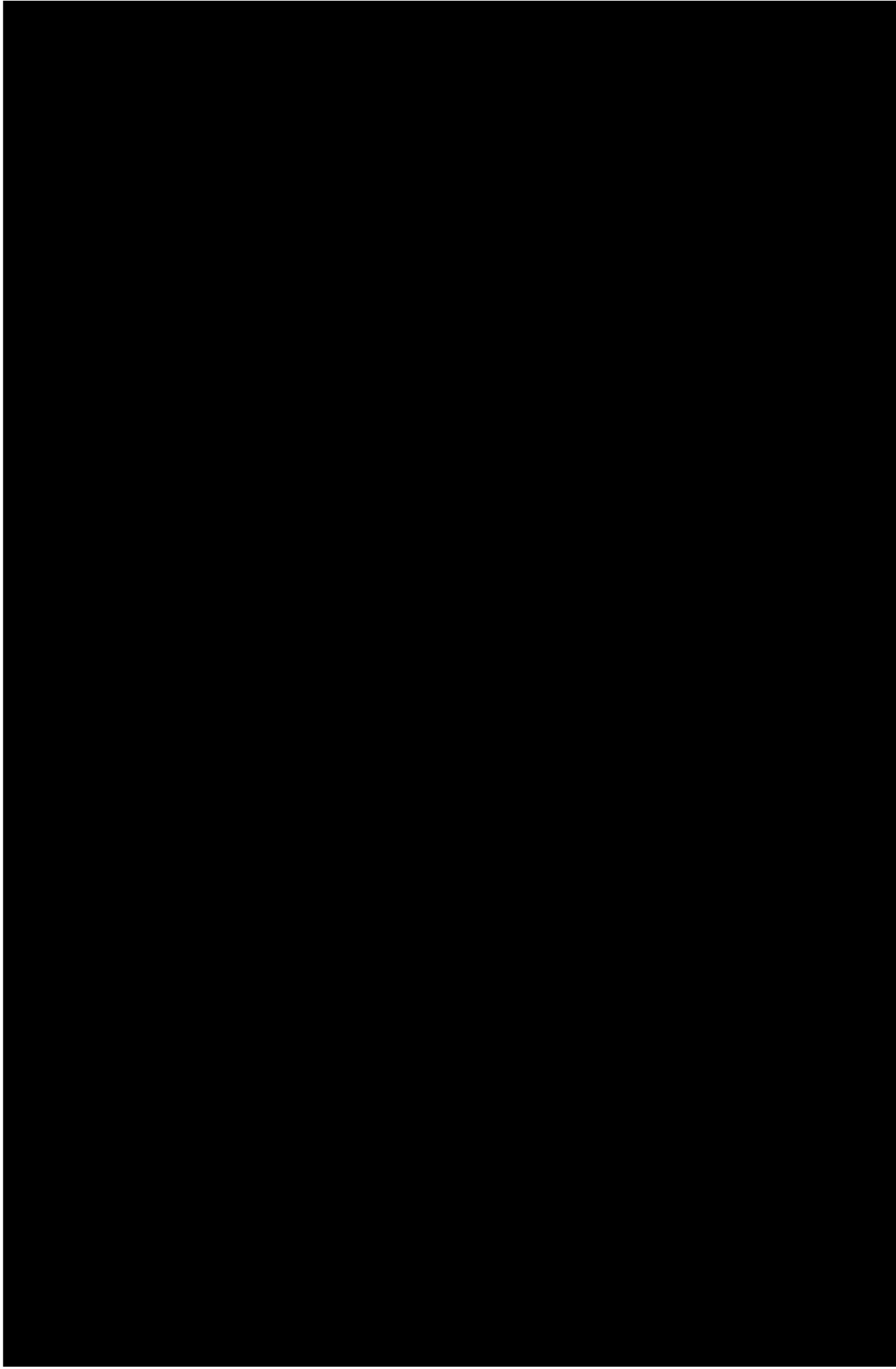
Specific impacts on the individual are considered to be across a spectrum, and each risk has many 10s of potential impact scenarios across that spectrum. For example, the impact on an individual could range from no impact / not noticed (1), mild annoyance / minimal action (2) through the spectrum to other more profound harms (5); these correlate to the Severity of Harm rating and for the risk table below, a reasonable worst-case scenario has informed the rating.

In almost all of the scenarios a breach of confidentiality to one of more people is likely, however risks such as to the rights and freedoms of the data subject are significantly less likely.

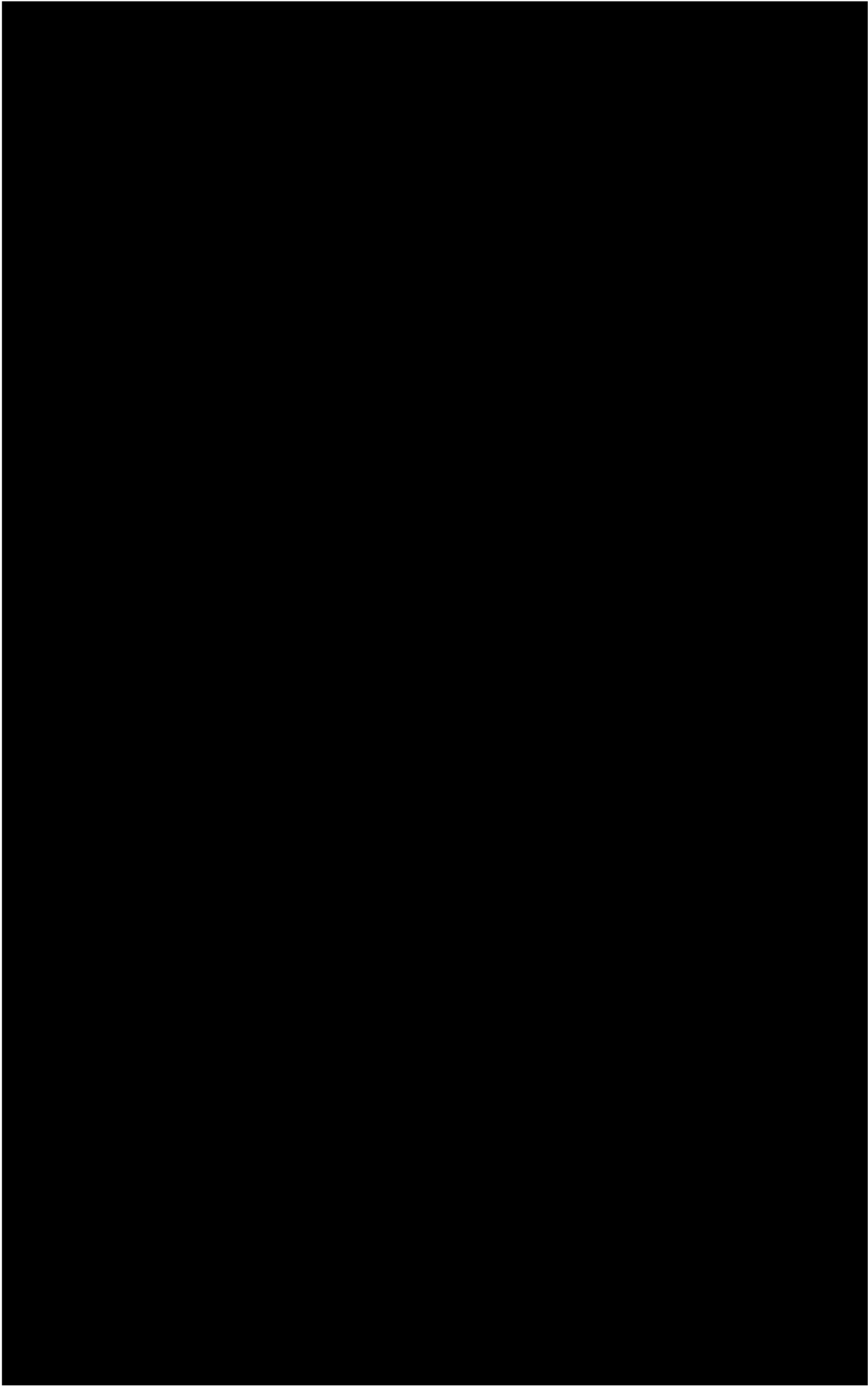
Table 1 – Risks and Mitigations associated with Health and Social Care Staff processing service user data through encompass				Mitigate Risks		
Assess Risks			Overall Risk (use Matrix, to calculate overall risk) Low Medium High	List the various controls that have been or will be put in place to mitigate the risk prior to commencement PLEASE ENSURE YOUR MITIGATION ADDRESSES THE RISK	Effect on risk Reduced Or Accepted* (*Select 'Accepted' where 'Overall risk' is rated as 'Low')	Residual risk Low Medium High
Describe below any specific data protection risks and nature of potential impact on individuals Include associated compliance as necessary	Likelihood of occurrence 1. Rare - This will probably never happen/recur 2. Unlikely - Do not expect it to happen/recur but it may do so 3. Possible - Might happen or recur occasionally 4. Likely - Will probably happen/recur, but it is not a persisting issue/circumstances 5. Almost Certain - Will undoubtedly happen/recur on a frequent basis	Severity of harm (if occurred) 1. Insignificant 2. Minor 3. Moderate 4. Major 5. Catastrophic				
(See Appendix 3 for examples). Please separate your risks out on separate rows			Refer to HSC Risk Matrix above ENTER NUMBERS BELOW			

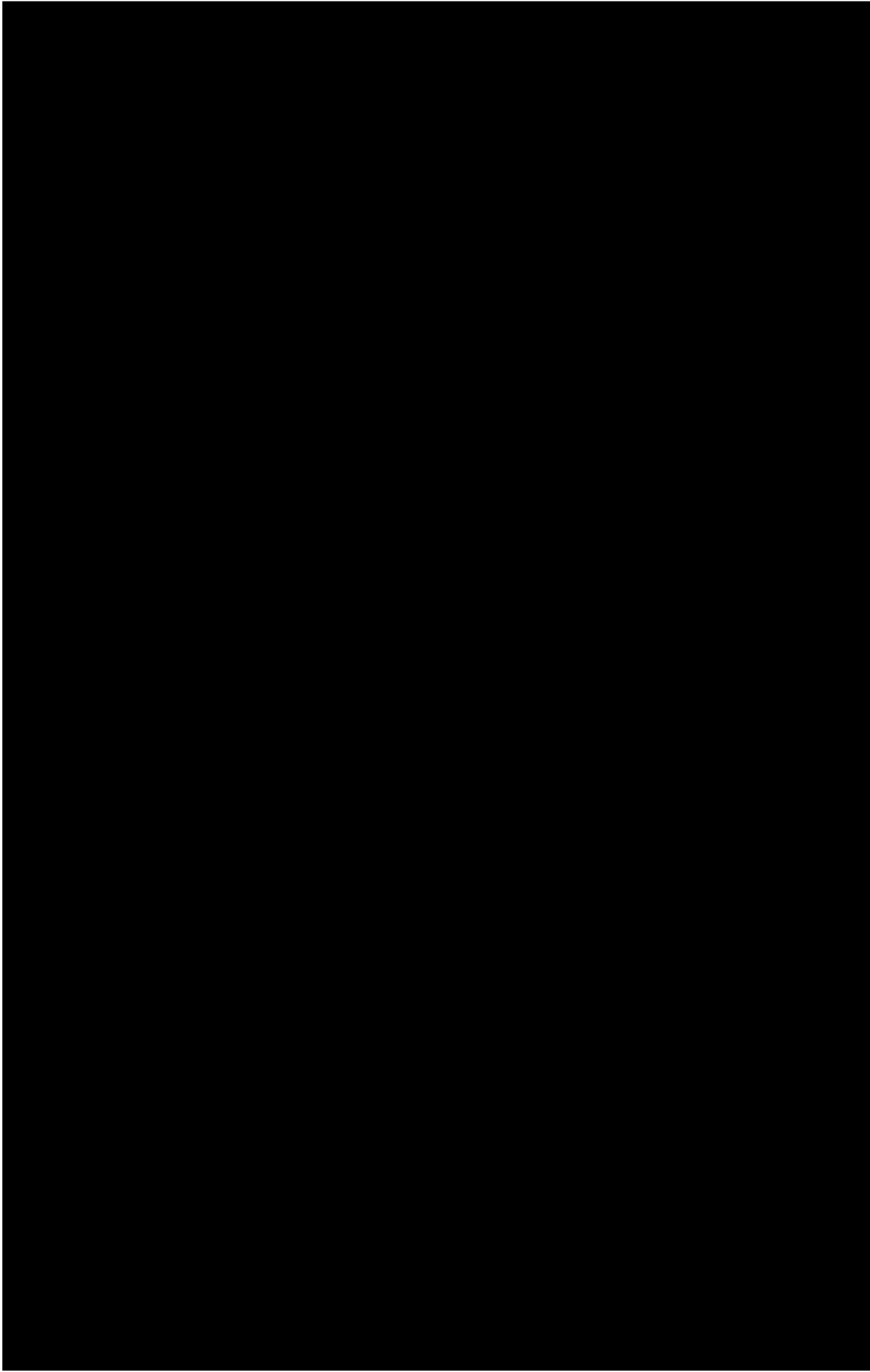


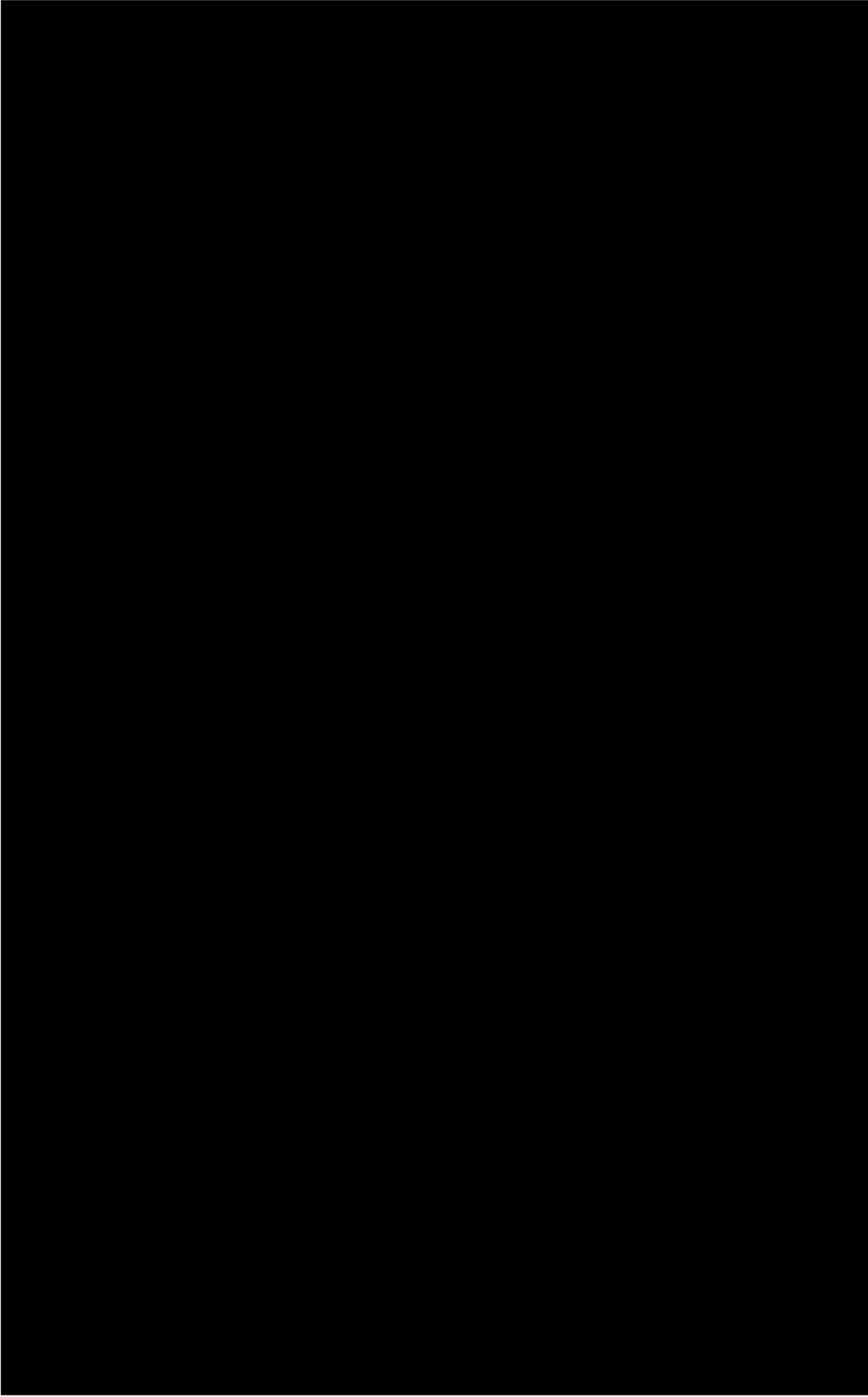


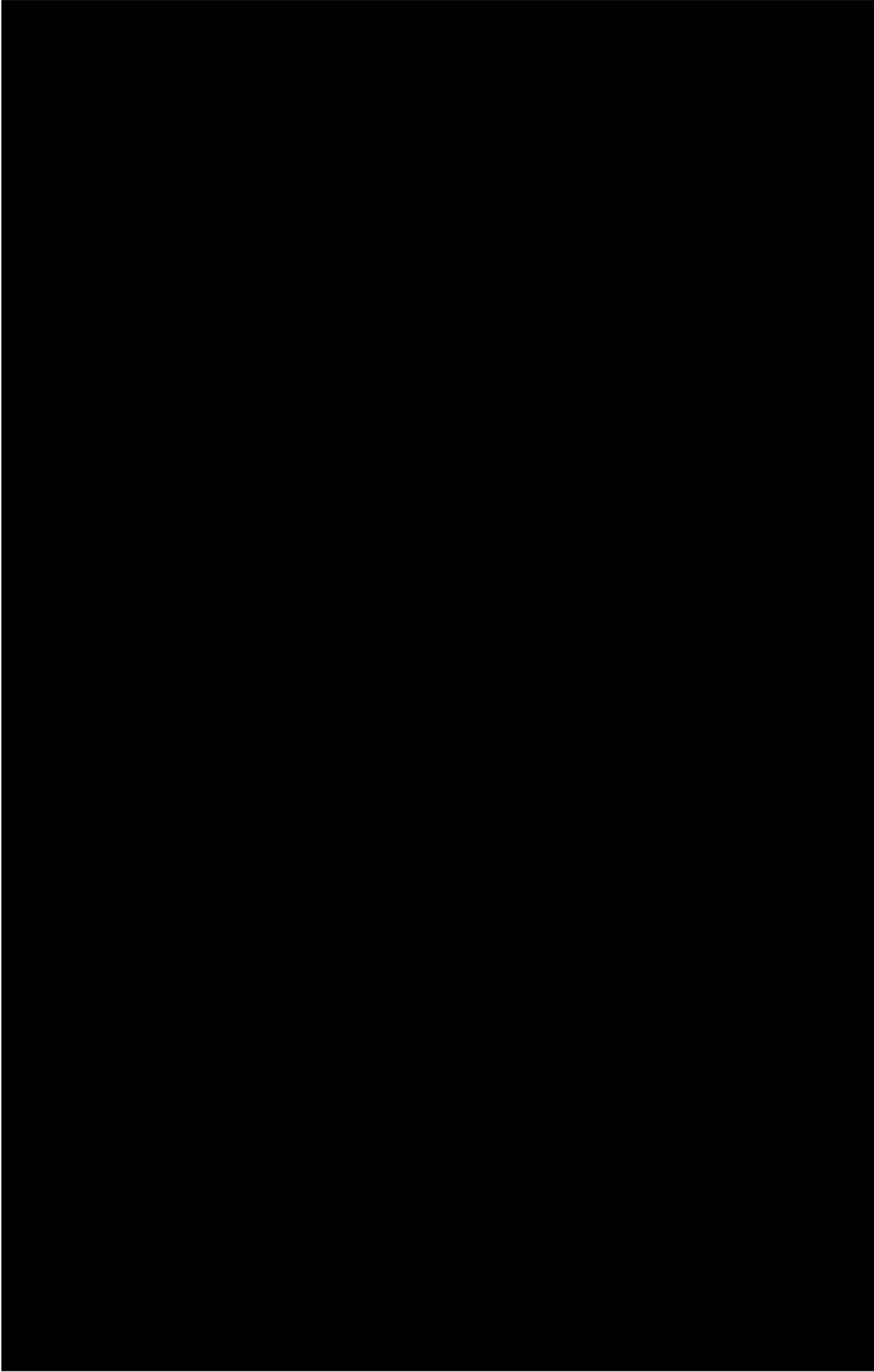


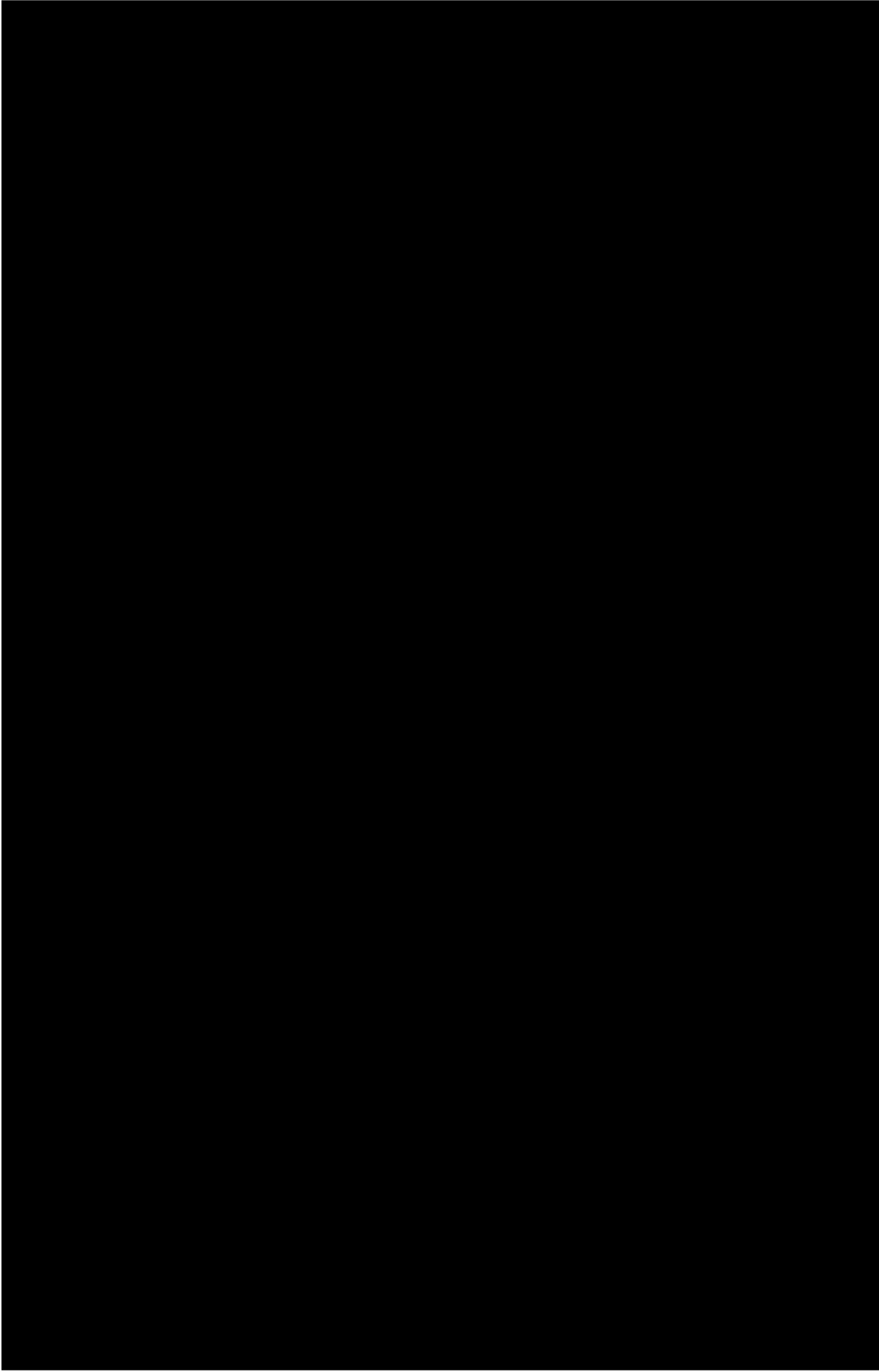
[REDACTED]

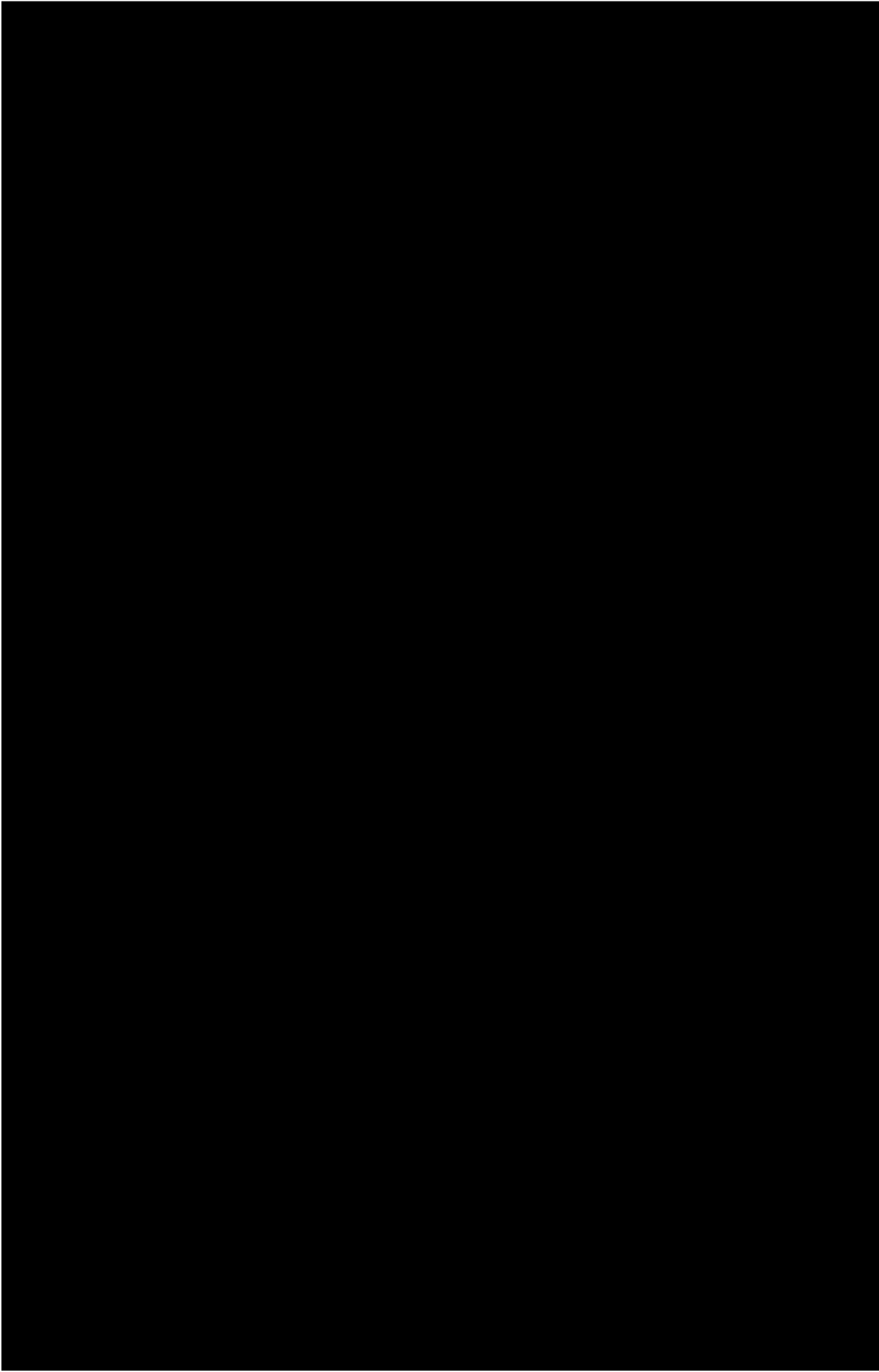


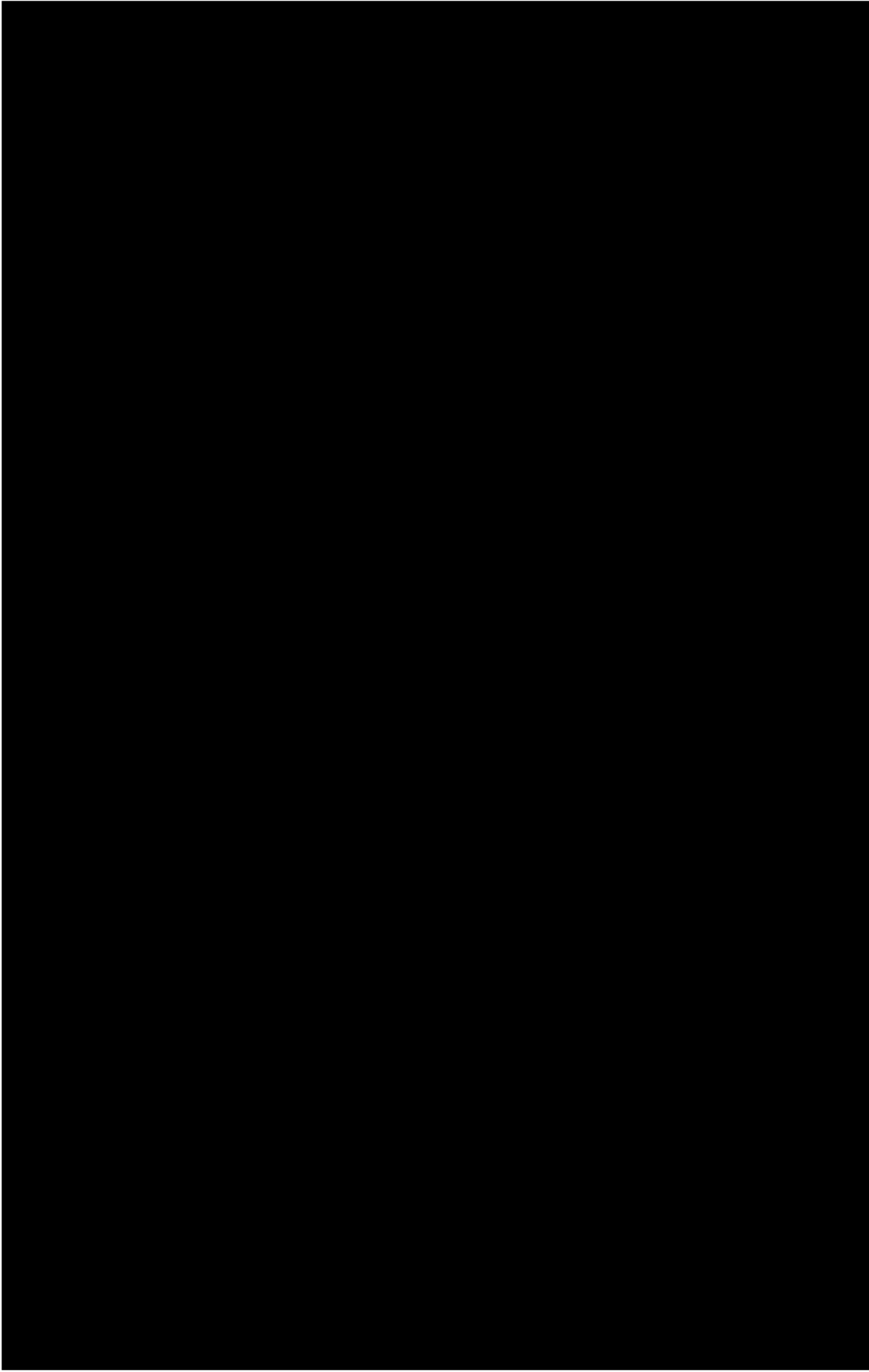


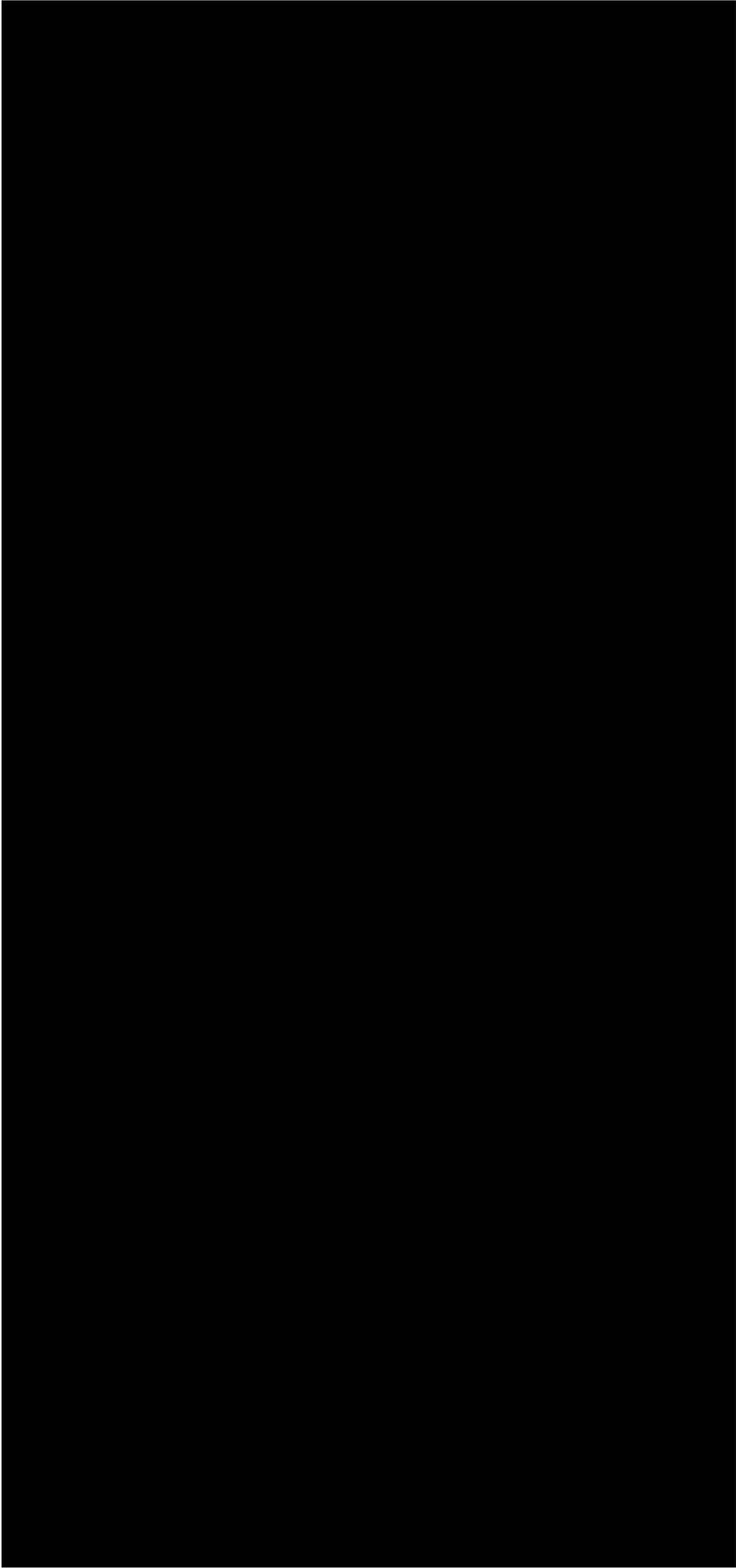












Add additional rows as required.

*** As per Step 10 please ensure the contract or relevant sharing agreement contains data protection clauses and covers the risks identified above**

Appendices

Appendix A

[REDACTED]

Appendix B

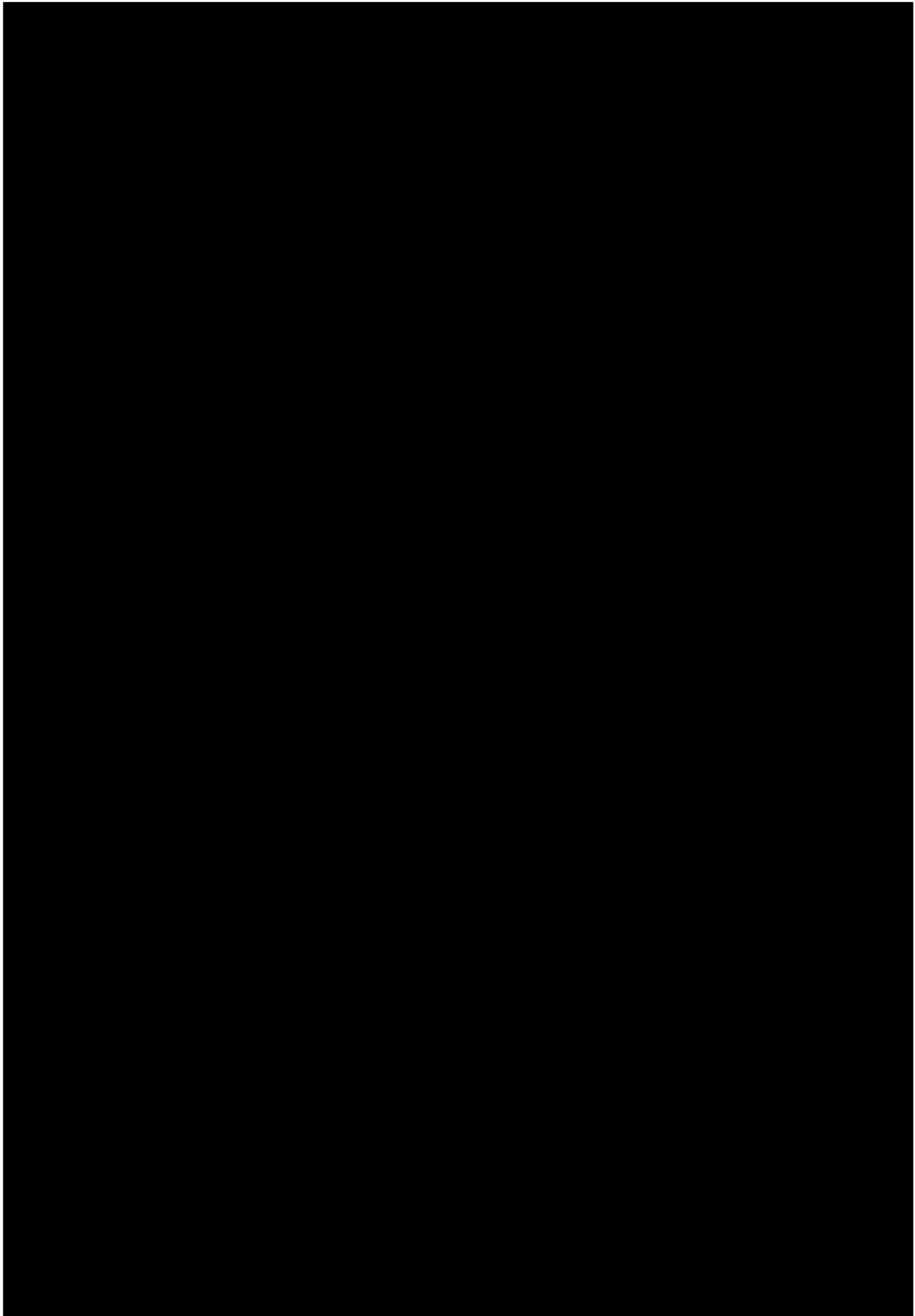
[REDACTED]

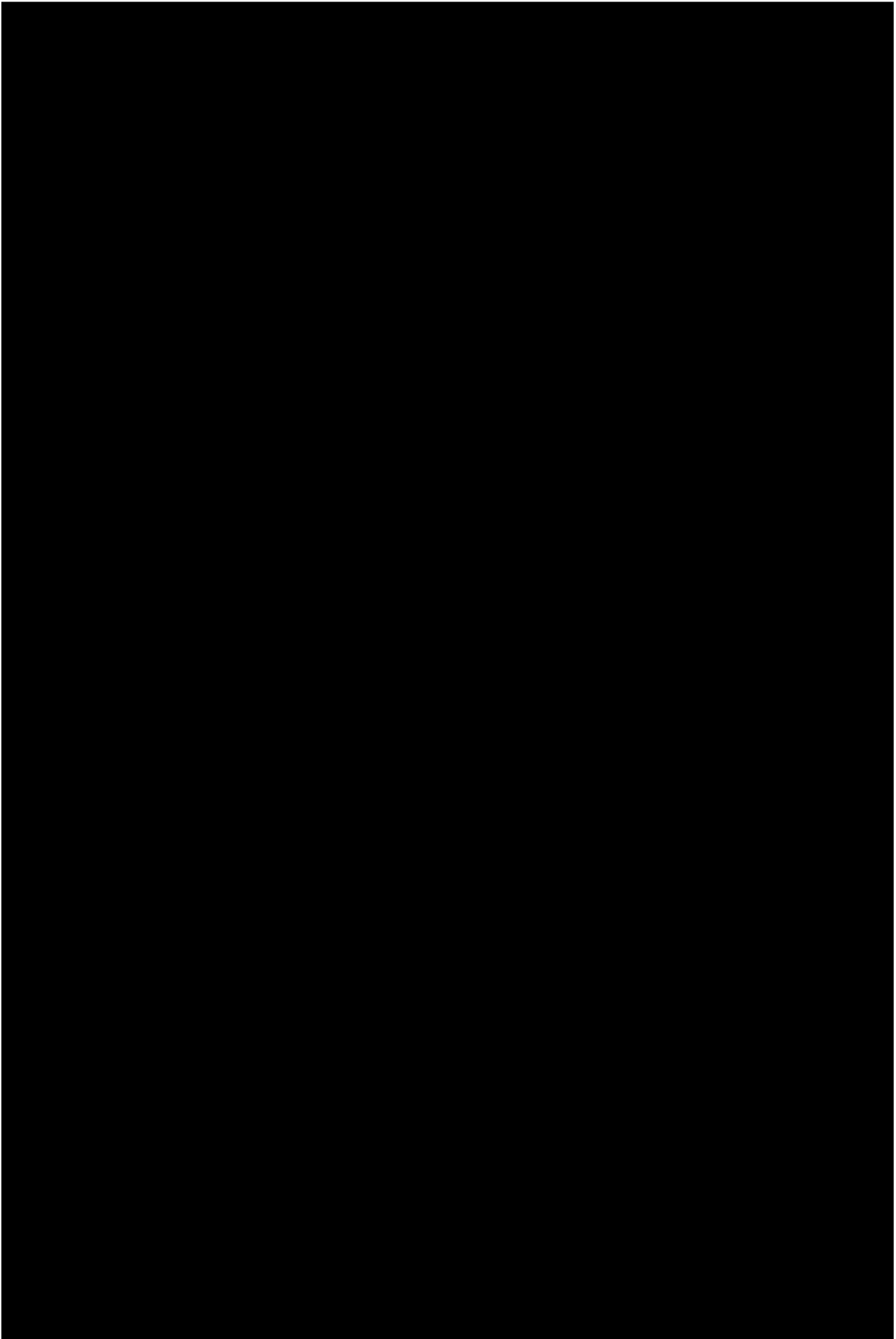
Appendix C

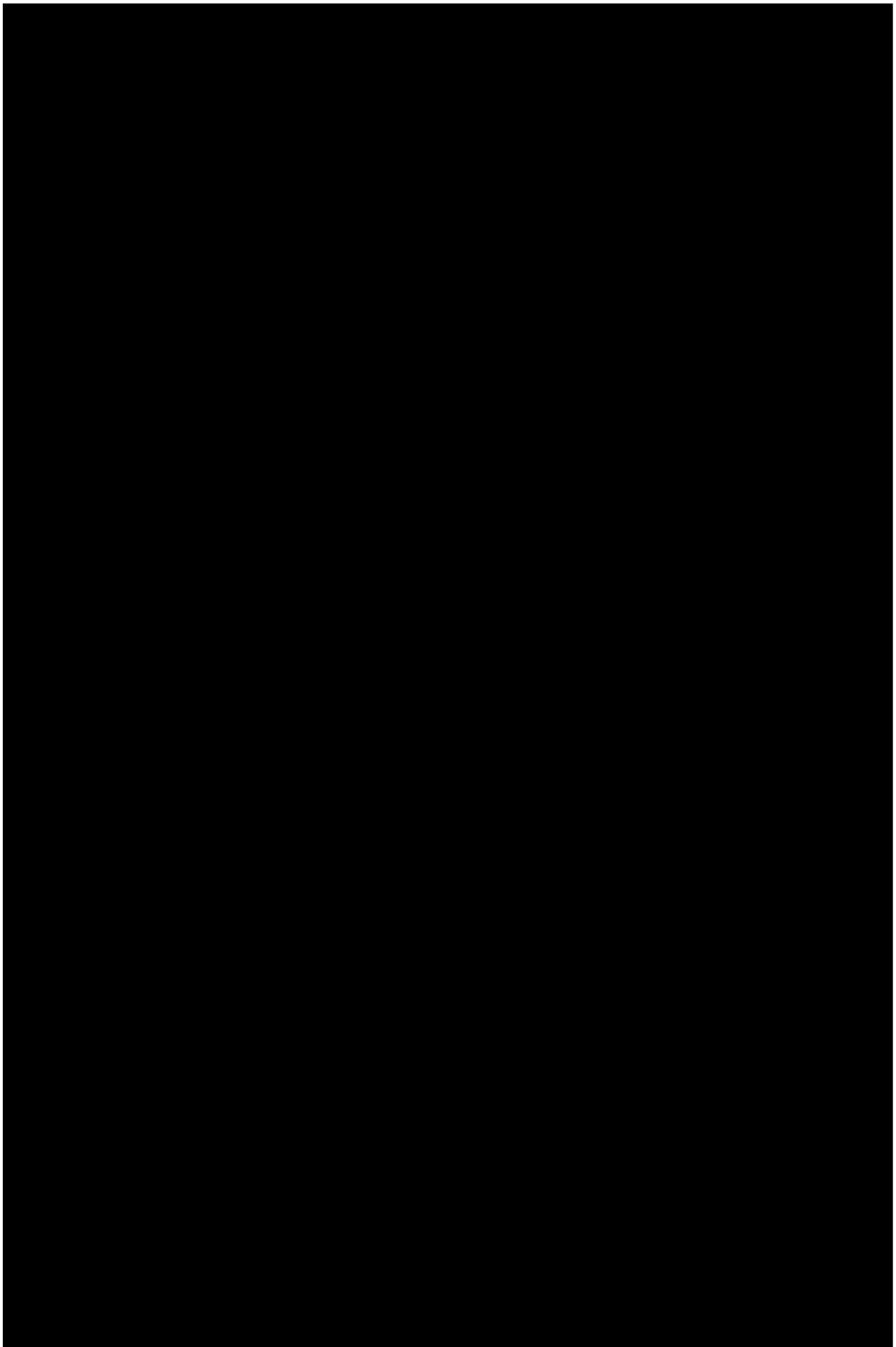
[REDACTED]

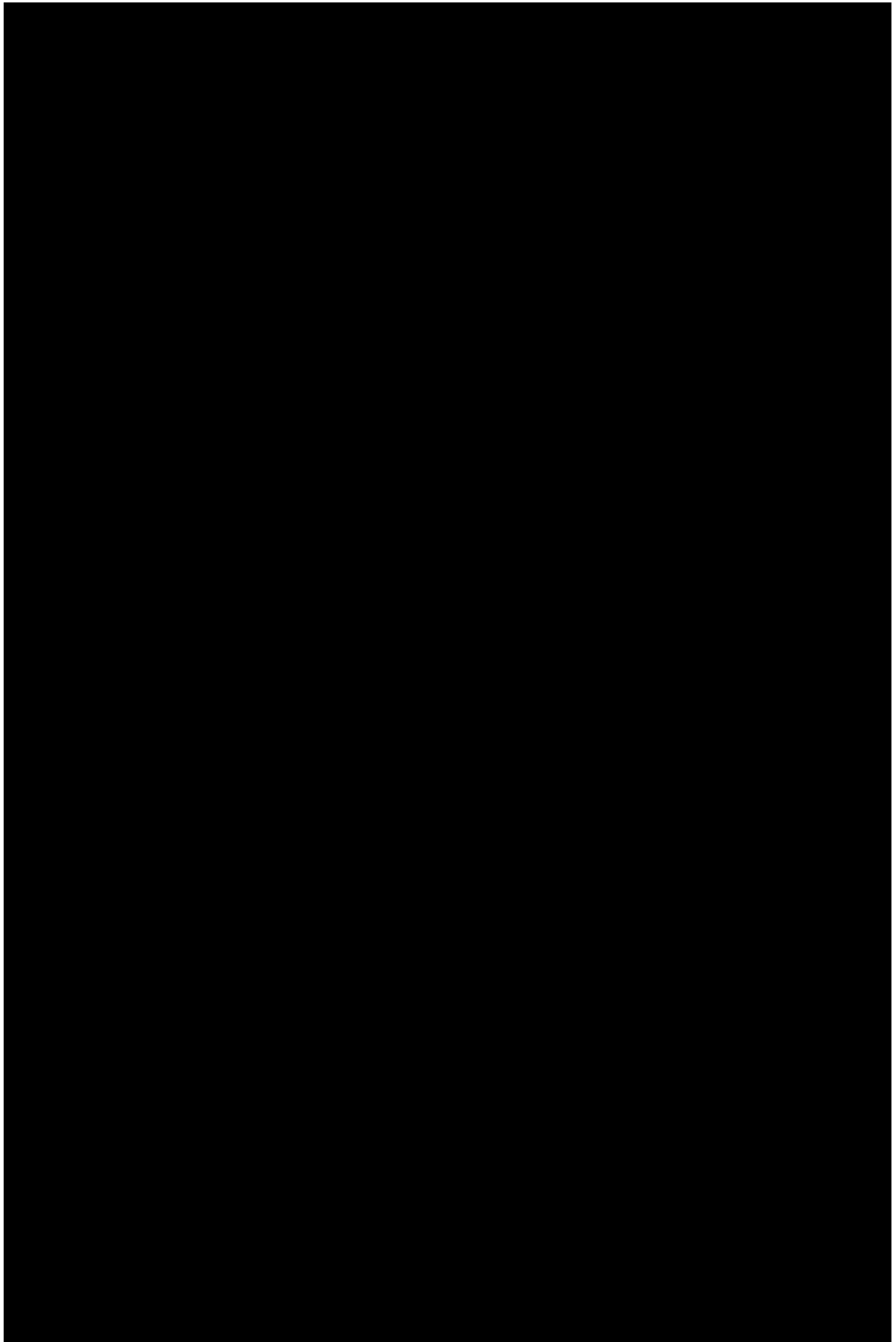
Appendix D

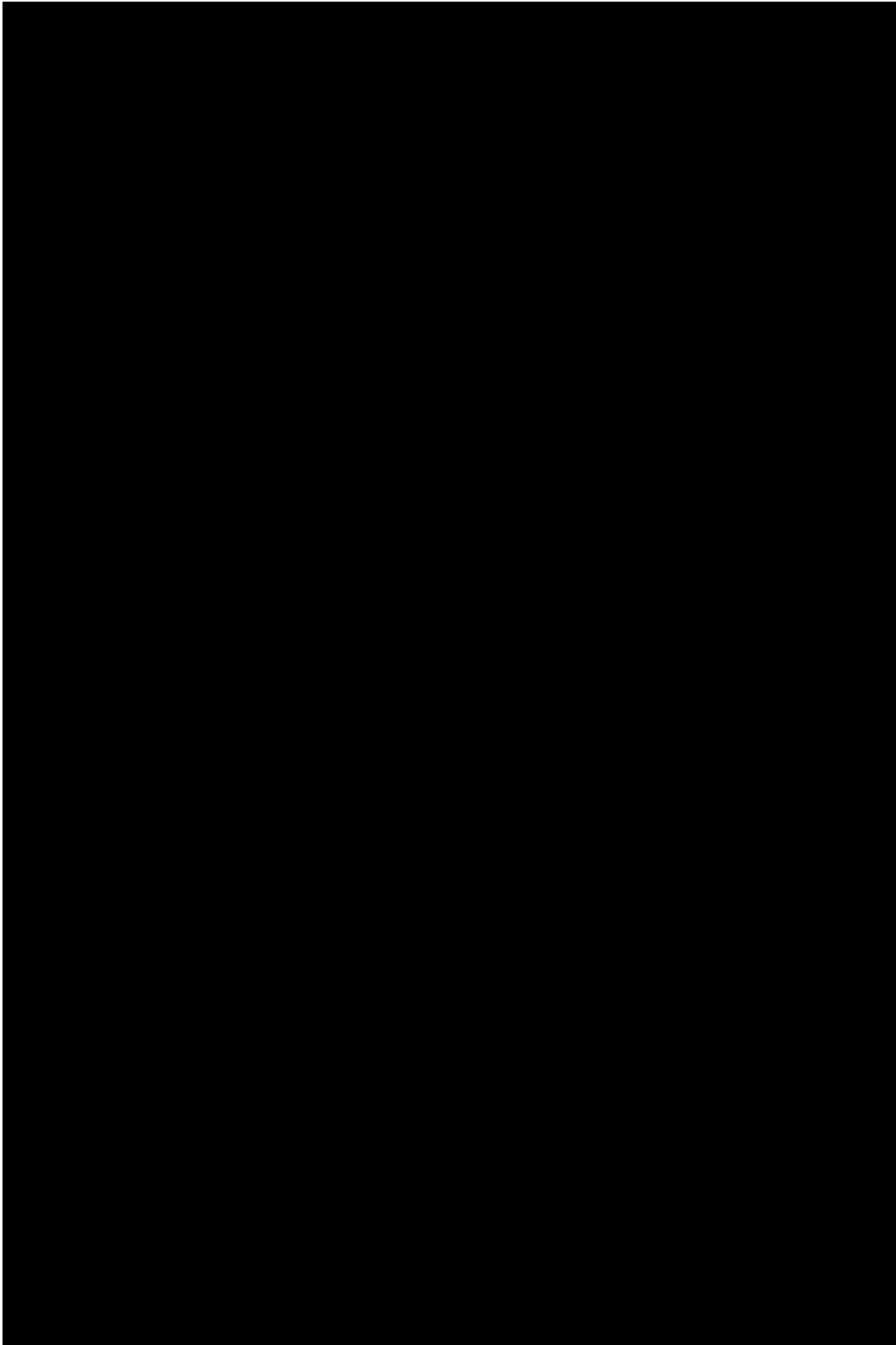
[REDACTED]

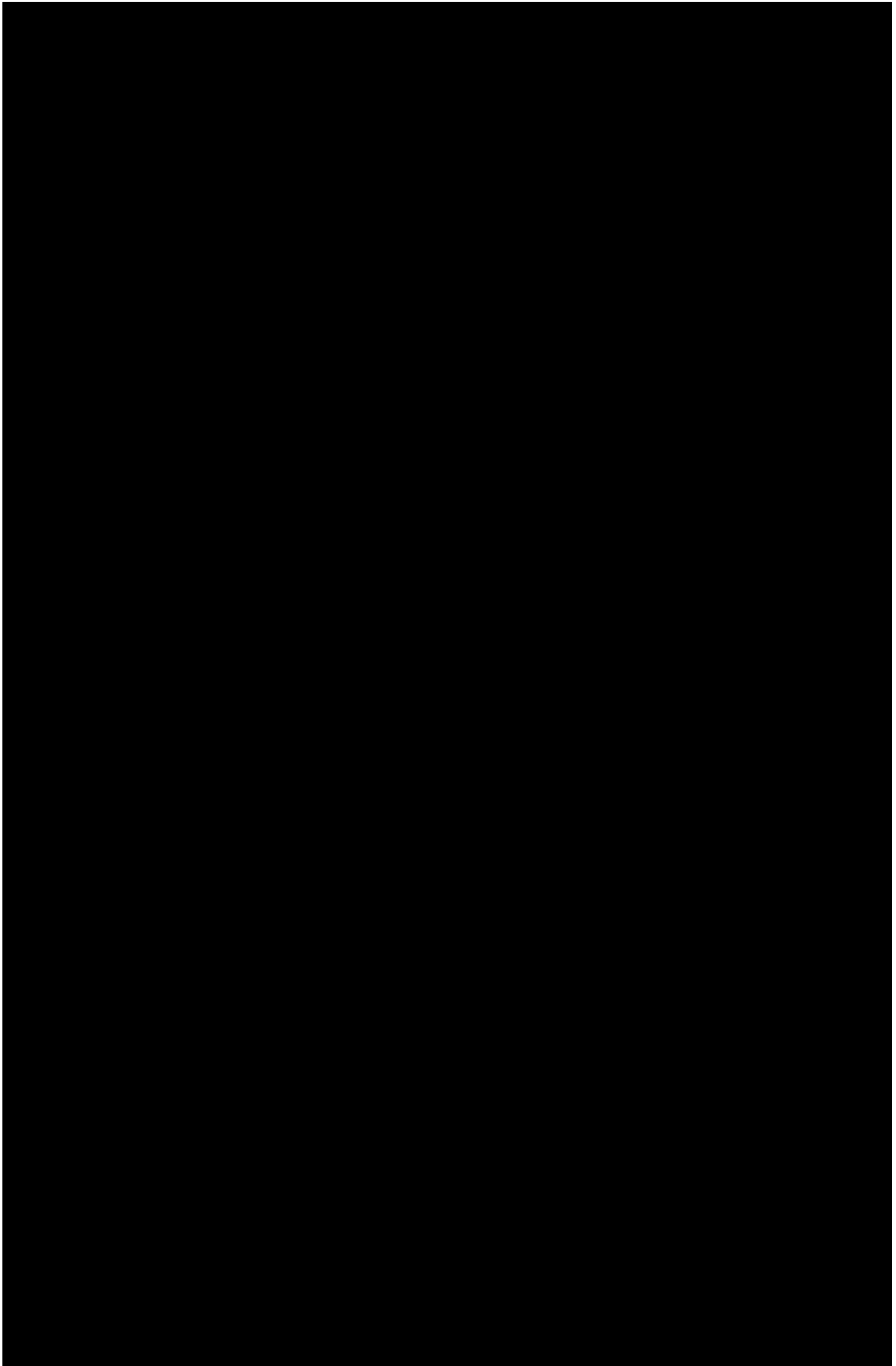












Appendix B

Access to the data is strictly controlled and limited to:

- **HSCNI Staff:** Healthcare professionals and administrative staff who require access to perform their job roles. Access will be role-based and proportionate to the responsibilities of the staff member.
- **Third Parties:** Such as suppliers and support organisations. Data sharing agreements need to remain current to ensure compliance with data protection laws.
- **Affiliate Staff:** Authorised personnel from provider, , relevant regulators, regional bodies and independent and private non-HSCNI healthcare providers, such as GP Practices, hospices, SPPG, PHA, DoH and RQIA to ensure delivery of care and compliance with reporting and statutory obligations. [REDACTED]

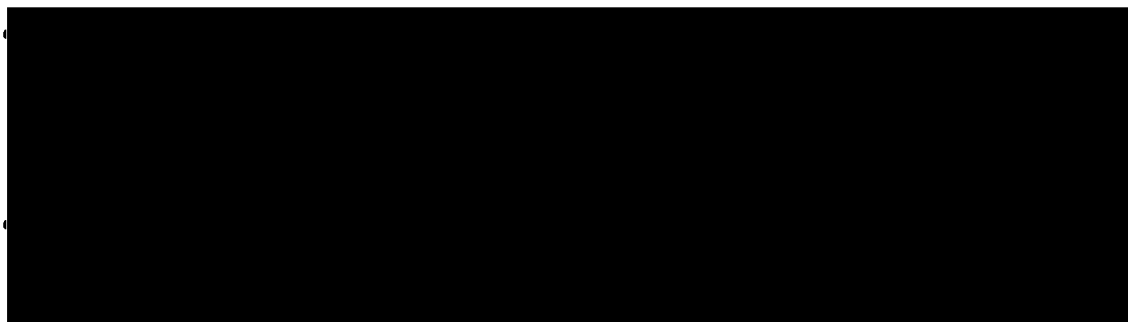
Access to records, features and data items are secured [REDACTED] through RBAC – Role Based Access Control).

This appendix describes the scenarios identified during the implementation of HSC encompass/Epic that require patient confidentiality considerations beyond the usual user security and access settings expected of an electronic health and social care record (EHCR).

It also describes the Epic tools and functionality that allow sensitive patient information to be protected, and how these are applied to the scenarios identified.

The work is underpinned by several fundamental principles.

- The Health and Social Care Record is confidential, and this is applicable to all sections whether marked 'sensitive' or not
- All staff are bound by UK statute and local policy on confidentiality
- Processes for the management of confidentiality will be straight forward and not open to interpretation
- Where possible the eDG seeks to improve on [REDACTED] and not complicate workflows
- Where possible the eDG will identify best practice in other Trusts as guidance

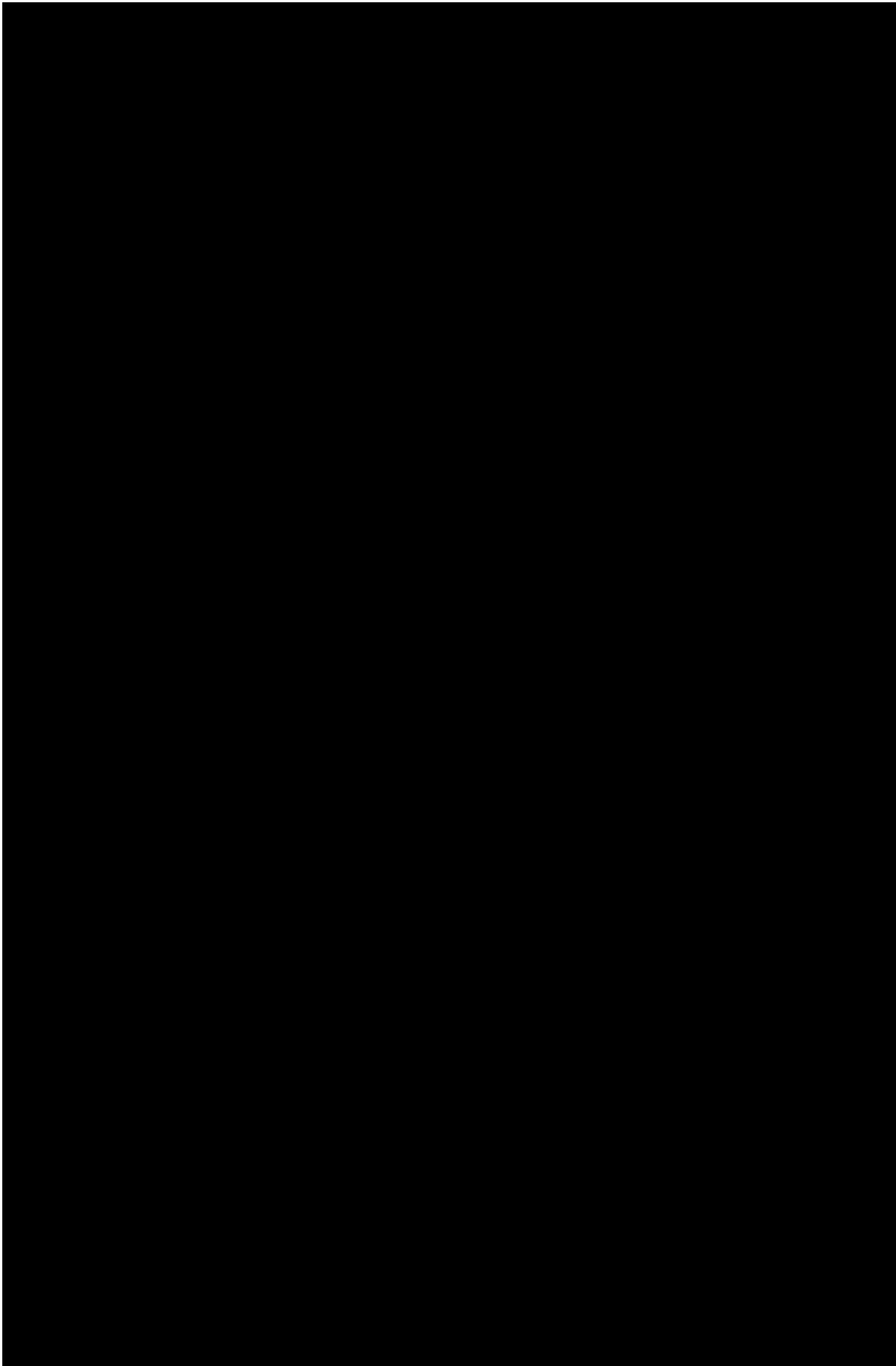


[REDACTED]

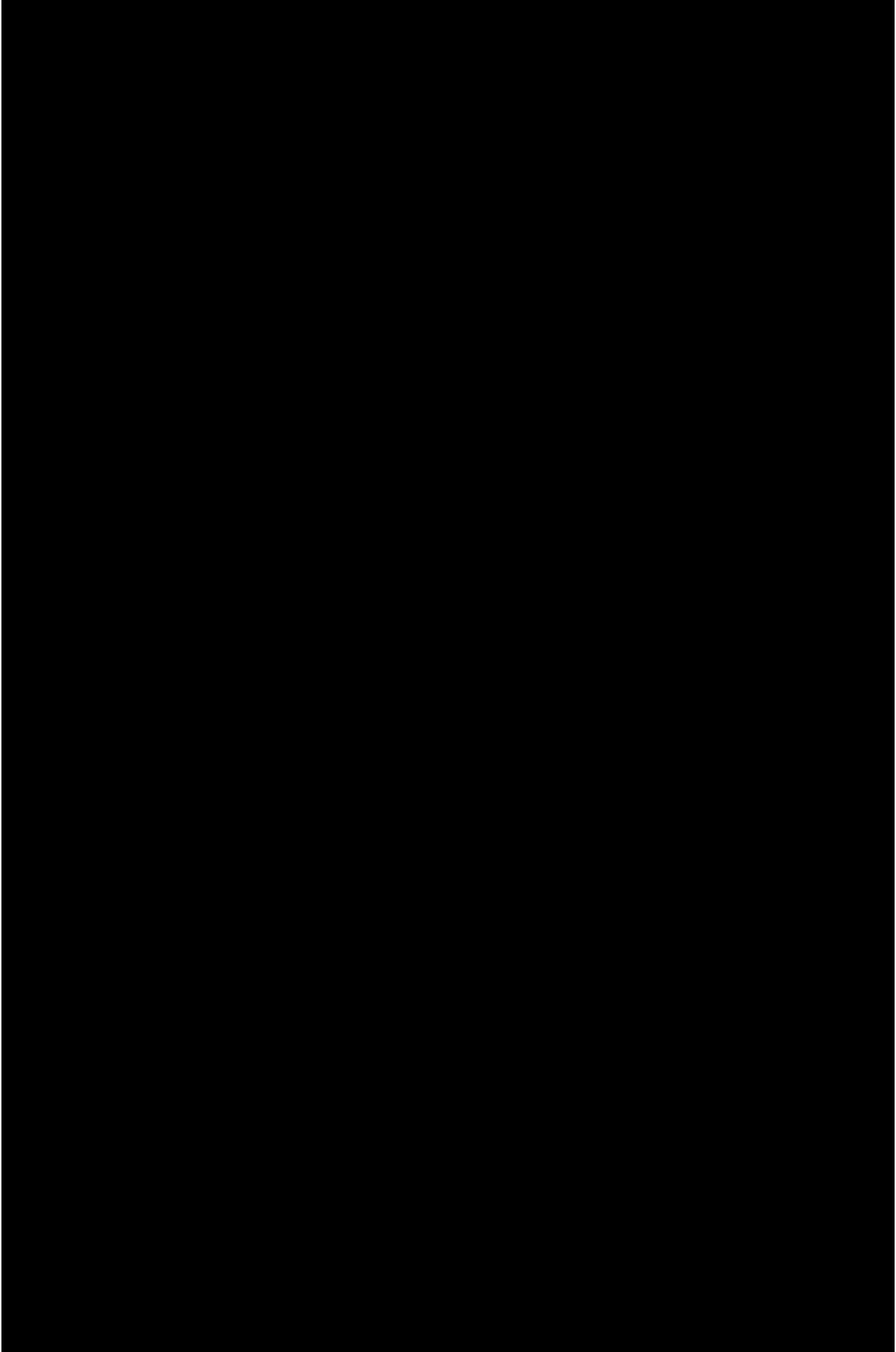
There are a range of privacy controls, tools and features in place as outlined below. Staff are provided training in these areas, and additional assistive materia [REDACTED]

[REDACTED]

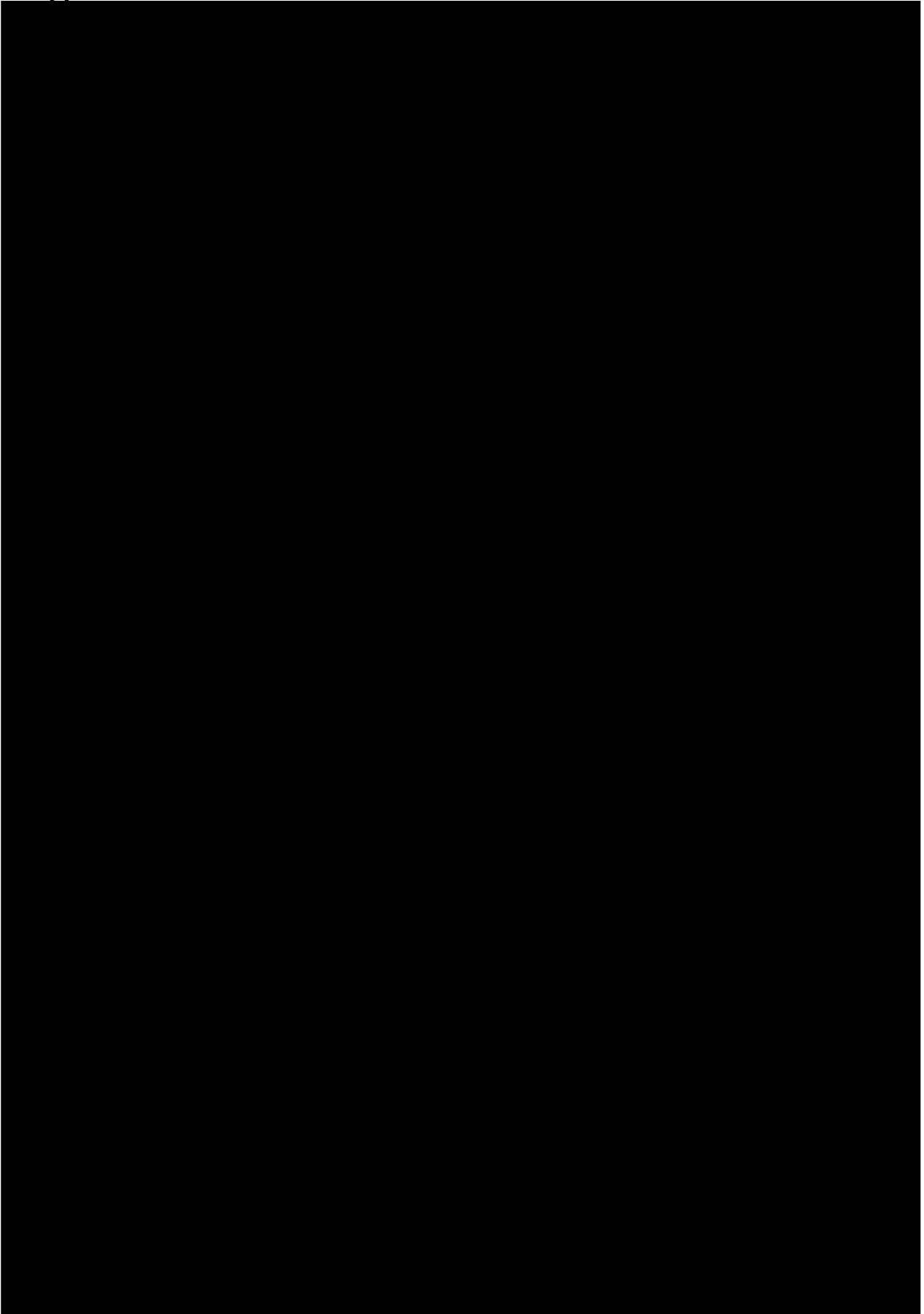
[REDACTED]

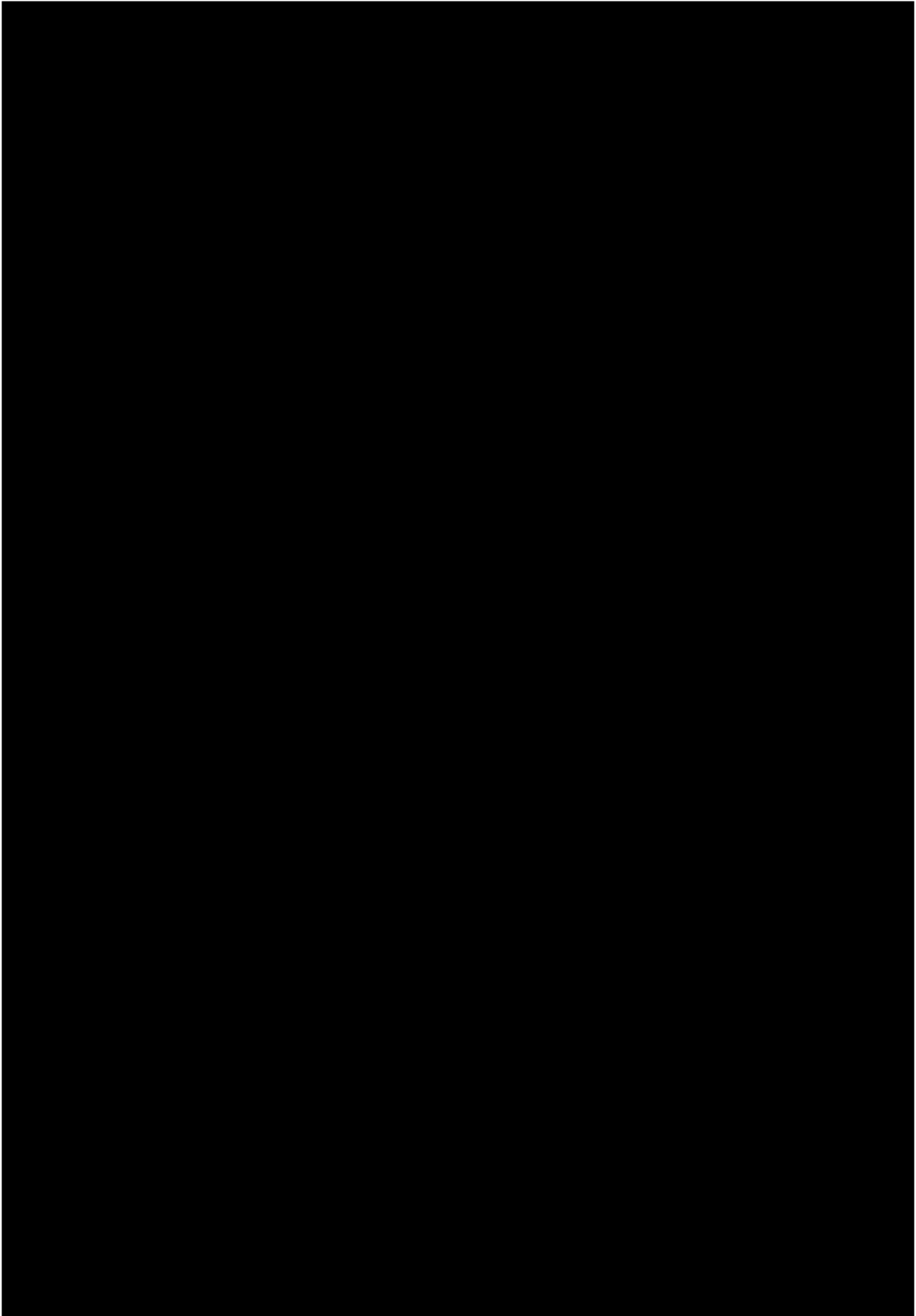


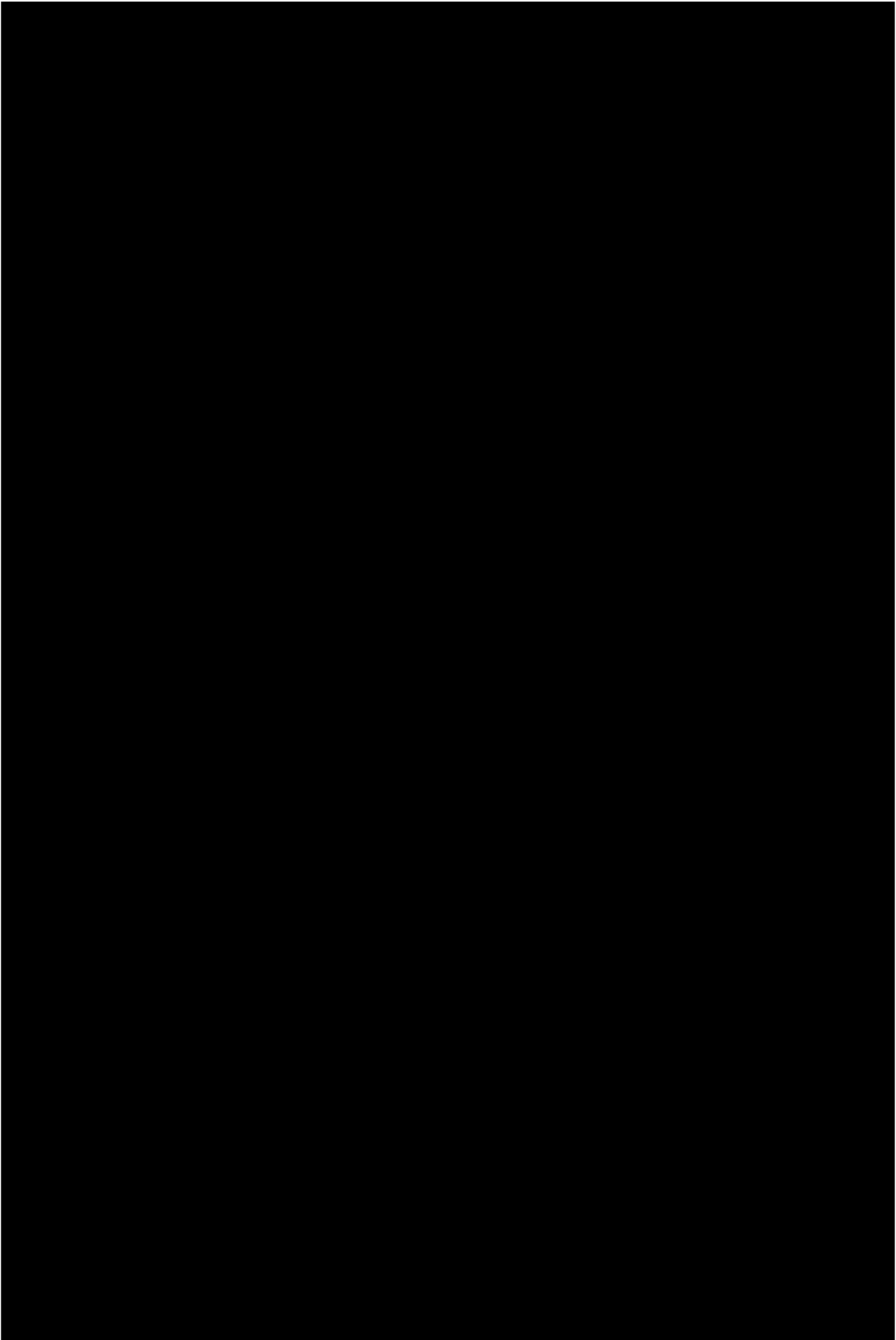
Appendix C



Appendix D







Step 12. SIGN OFF and record outcomes
a. Project Lead / Service Lead: In signing this DPIA I confirm the following: <i>I am satisfied that this is an accurate reflection of how the service will be provided and the expected data flows. I have consulted with all necessary stakeholders and sought the views of others as required (including IG and ICT). I have incorporated relevant advice into this document and into the plans for delivery of the service. Where necessary, I will ensure any additional documentation is put in place, such as a Privacy Notice to inform service users of how their personal data is to be processed; and/or any required Contracts or Agreements to cover data sharing with third party organisations.). I will ensure the contract or alternative information sharing agreement will contain specific data protection clauses which address the risks identified.</i> <i>I confirm that I will keep the DPIA under review and will update this document with any substantive changes to the data processing activities or data flows.</i>
Any additional comments:
Signature:  Full Name: [REDACTED] Job Title/Role: Senior Programme Manager Date Signed: 25/03/2025

b. SE HSCT Data Protection Officer (DPO) advice and sign-off

Summary of DPO advice:

Signature:

Signed by:

[REDACTED]

Full Name:

Job Title/Role: Head of InfoGov

Date Signed: 15/10/2025

c. SE HSCT Senior Information Risk Owner (SIRO) - Final Approval

I have considered the data protection aspects of this project and any DPO comments (above). I accept any residual risks and will ensure the various controls outlined to mitigate the identified risks are put in place prior to commencement. I will ensure that no data processing will take place until this DPIA has been completed and signed. I will ensure that this DPIA is reviewed and updated if the data processing changes. I will ensure that all staff involved in the processing of personal data are aware of their responsibilities to complete mandatory Information Governance training. I will arrange for this new system/process to be added to the Information Asset Register (IAR) and/or Risk Register.

Any additional comments:

Signature:

DocuSigned by:

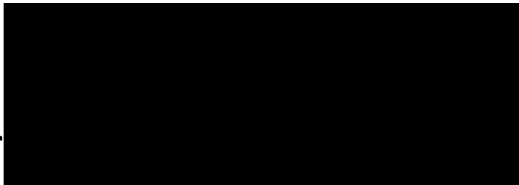
[REDACTED]

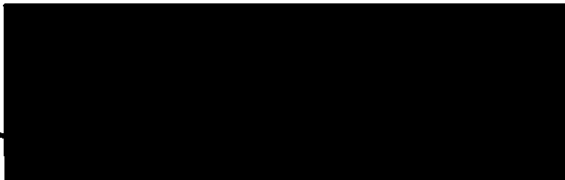
Full Name:

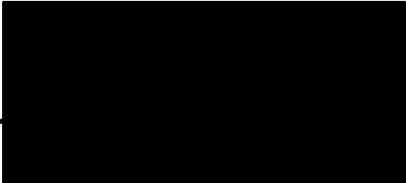
Job Title/Role: Director Planning Performance

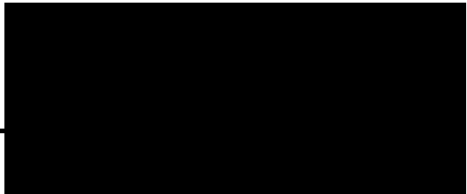
Date Signed: 15 10 2025

--

d. Belfast HSCT Data Protection Officer (DPO) advice and sign-off
Summary of DPO advice:
Signature:
DocuSigned by: 
Full Name: Cathy Cole
Job Title/Role: Senior Mgr Information Governance
Date Signed: 30/10/2025

e. Belfast HSCT Senior Information Risk Owner (SIRO) - Final Approval
<i>I have considered the data protection aspects of this project and any DPO comments (above). I accept any residual risks and will ensure the various controls outlined to mitigate the identified risks are put in place prior to commencement. I will ensure that no data processing will take place until this DPIA has been completed and signed. I will ensure that this DPIA is reviewed and updated if the data processing changes. I will ensure that all staff involved in the processing of personal data are aware of their responsibilities to complete mandatory Information Governance training. I will arrange for this new system/process to be added to the Information Asset Register (IAR) and/or Risk Register.</i>
Any additional comments:
Signature:
Signed by: 
Full Name: Alastair Campbell
Job Title/Role: Director PPI
Date Signed: 05/12/2025

f. Northern HSCT Data Protection Officer (DPO) advice and sign-off
Summary of DPO advice:
Signature:
Signed by:

Full Name: [Redacted]
Job Title/Role: Head of IG/DPO
Date Signed: 05/01/2026

g. Northern HSCT Senior Information Risk Owner (SIRO) - Final Approval <i>I have considered the data protection aspects of this project and any DPO comments (above). I accept any residual risks and will ensure the various controls outlined to mitigate the identified risks are put in place prior to commencement. I will ensure that no data processing will take place until this DPIA has been completed and signed. I will ensure that this DPIA is reviewed and updated if the data processing changes. I will ensure that all staff involved in the processing of personal data are aware of their responsibilities to complete mandatory Information Governance training. I will arrange for this new system/process to be added to the Information Asset Register (IAR) and/or Risk Register.</i>
Any additional comments:
Signature:
Signed by:

Full Name: [Redacted]
Job Title/Role: Director SPPICT / SIRO
Date Signed: 5/1/2026

Summary of DPO advice:

Signature:

DocuSigned by:

Full Name: [REDACTED]

Job Title/Role: Assistant Director of Informatics

Date Signed: 13/01/2026

I have considered the data protection aspects of this project and any DPO comments (above). I accept any residual risks and will ensure the various controls outlined to mitigate the identified risks are put in place prior to commencement. I will ensure that no data processing will take place until this DPIA has been completed and signed. I will ensure that this DPIA is reviewed and updated if the data processing changes. I will ensure that all staff involved in the processing of personal data are aware of their responsibilities to complete mandatory Information Governance training. I will arrange for this new system/process to be added to the Information Asset Register (IAR) and/or Risk Register.

Any additional comments:

Signature:

Signed by:

Full Name:

Job Title/Role: Director of Planning, Performance & Info

Date Signed: 14/01/26

j. Western HSCT Data Protection Officer (DPO) advice and sign-off
Summary of DPO advice:
Signature:
Signed by:

Full Name: 
Job Title/Role: Head of Information Governance and Records Management
Date Signed: 09/03/2026

k. Western HSCT Senior Information Risk Owner (SIRO) - Final Approval
<i>I have considered the data protection aspects of this project and any DPO comments (above). I accept any residual risks and will ensure the various controls outlined to mitigate the identified risks are put in place prior to commencement. I will ensure that no data processing will take place until this DPIA has been completed and signed. I will ensure that this DPIA is reviewed and updated if the data processing changes. I will ensure that all staff involved in the processing of personal data are aware of their responsibilities to complete mandatory Information Governance training. I will arrange for this new system/process to be added to the Information Asset Register (IAR) and/or Risk Register.</i>
Any additional comments:
Signature:
Signed by:

Full Name: 
Job Title/Role: DIRECTOR OF PLANNING, PERFORMANCE & CORPORATE SERVICES
Date Signed: 9 MARCH 2026

Please return a copy of the final signed DPIA to the Information Governance Department

Appendix 1 - Data Protection Principles

The data protection principles are contained in the UK GDPR and require that personal information must be:

a) Processed lawfully, fairly and in a transparent manner in relation to the data subject - (Lawfulness, Fairness and transparency). There must be valid grounds under the UK GDPR (known as a 'lawful basis') for collecting and using personal data and you must not do anything with the data in breach of any other laws. Personal data must be processed in a way that is fair and not unduly detrimental, unexpected or misleading to the individuals concerned. You must be clear, open and honest with people from the start about how you will use their personal data.

b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. (Purpose limitation)

c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed - (data minimisation)

d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay – (Accuracy)

e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (Storage Limitation)

f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures - (Integrity and Confidentiality)

In accordance with Article 5(2) of the UK GDPR the data controller shall be responsible for, and through its policies, procedures and protocols will demonstrate compliance with the Data Protection Principles listed above (**overarching principle of Accountability**).

Appendix 2 – Lawful Basis for processing Personal Information and Special Category Information

You must have a valid lawful basis in order to process personal data in compliance with Article 6 of UK GDPR.

If you are processing special category data*, you also need to identify a further special category condition in compliance with Article 9 of UK GDPR.

You should document your lawful basis for processing and your special category condition so that you can demonstrate compliance and accountability

The lawful bases for processing are set out in **Article 6 of the UK GDPR**. At least one of these must apply whenever you process personal data:

- (a) Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.
- (b) Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
- (c) Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).
- (d) Vital interests:** the processing is necessary to protect someone's life.
- (e) Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
- (f) Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. *(NB. Please consult with your IG Department before using this as your lawful basis for processing personal data. This cannot be applied by a public authority processing data to perform its official / core function (e.g. processing data as part of the provision of health or social care) however may be relevant for non-core functions such as HR)*

Special category data is personal data that needs more protection as it is more sensitive than basic personal data. The UK GDPR defines special category data as:

- personal data revealing **racial or ethnic origin**;
- personal data revealing **political opinions**;
- personal data revealing **religious or philosophical beliefs**;
- personal data revealing **trade union membership**;
- **genetic data**;
- **biometric data** (where used for identification purposes);
- data concerning **health**;
- data concerning a person's **sex life**; and
- data concerning a person's **sexual orientation**.

Article 9 lists the conditions for processing special category data:

- (a) Explicit consent
- (b) Employment, social security and social protection (if authorised by law)
- (c) Vital interests
- (d) Not-for-profit bodies
- (e) Made public by the data subject
- (f) Legal claims or judicial acts
- (g) Reasons of substantial public interest (with a basis in law)
- (h) Health or social care (with a basis in law)
- (i) Public health (with a basis in law)
- (j) Archiving, research and statistics (with a basis in law)

See the Information Commissioner's Office (ICO) website (links below):

- For more detail on each lawful basis for processing personal data

<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/>

- For more detail on the additional conditions for processing special category (sensitive) personal data

<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/>

Appendix 3 - Examples of possible risks include: Please note that not all these risks are applicable to every project, nor is this list exhaustive. **Please ensure that the risks you list in step 6 are relevant to your project.**

DP Principle (see App 1)	Example Risk	Example Mitigation
Lawfulness, Fairness and Transparency	Inadequate Communication – individuals not informed of how the HSC organisation will use their data The form of processing may raise public concerns (e.g. using CCTV footage/audio recording function without informing staff/service users) Privacy notice, consent form, policies and processes not sufficient to cover lawful basis	Privacy Notice in place
		Staff and service users will be informed of the method of data collection and how the data is processed i.e. CCTV/audio recording notification
		Standard operating procedures/staff guidance/ HSC organisation or regional policy/privacy notices and consent forms to be drafted or reviewed in line with the project outcomes
Purpose Limitation	Risk of function creep – that the data is used for a purpose other than the one specified such as using data collected for health for targeted marketing purposes Third party processors/contractors using data for purpose not specified (e.g. marketing purposes)	Clearly defined purpose and limitations set out in information sharing agreement/contract. Review of internal SOP.
		Clearly defined roles and responsibilities included within Contract/Information Sharing Agreement
Data Minimisation	Collecting more data than is required to fulfil purpose	Use of pre-set data fields to ensure no information is collected than necessary
Accuracy:	Mechanisms not in place to ensure data quality/ accuracy to avoid an unintentional data breach or non-compliance.	Ensure all procedures and agreements around data checking are fit for purpose.
	Inappropriate linking/merging records	- Understanding whether system has capacity to link records and if this is appropriate - Ensure there are Data Quality policies and procedures in place
Storage Limitation	Retention – information being retained longer than necessary	- Standard operating procedures to be drafted or reviewed in line with Good Management/ Good Records - Ensure that data retention periods (reflective of GMGR) are outlined in contracts and information sharing agreements and mechanisms exist to manage this by the appropriate parties

	Personal information (manual and electronic records) held with no formal retention policy in place	- Standard operating procedures to be drafted or reviewed in line with Good Management/ Good Records - Ensure that appropriate procedures are in place for retention and disposal of these records
Integrity and Confidentiality (Security)	Risk from threat actors such as cyber criminals, hackers or disgruntled employees on system or cloud	
	Cyber-attack from unknown source received into the HSC organisation (e.g. opening attachment from unknown source which may contain virus)	
	Use of HSC organisation apps on personal devices without a known level of security	
	Risk when transferring information internally or externally that the information could be inappropriately disclosed during transfer due to inadequate control	
	Unauthorised access to information	
	Inadequate redaction/anonymisation of data	
	Loss of information due to inadequate controls around tracking/retrieval	- Adhering to data protection policy/guidance - Complying with UKGDPR and Good Management, Good Records to ensure appropriate measures in place to track and retrieve physical documents
	International transfers not monitored resulting information being transferred to servers based in countries without adequacy status or similar DP regime to UK/EU	

	Data loss risk due to system failure	
	Intended or accidental linking of data sets that may result in anonymised or pseudonymised data becoming personally identifiable.	
Accountability	Receiving organisation having inadequate framework to support data protection	Assurances to be provided by receiving organisation in the terms of the contract.
CCTV Risks	New surveillance methods may be an unjustified intrusion on privacy	Identify appropriate lawful basis and consult ICO if required to ensure data collection is justified
	Vulnerable people may be particularly concerned about the risks of identification	Appropriate privacy notice in place
	CCTV system is not used for its specified purpose.	• Purpose clearly specified in DPIA/Public Notices • Access to footage limited to only those who require it • Signage in place
	Inability to exercise information rights (e.g. SAR, FOI) if system does not have the functionality to pixelate images which are not the subject.	• Ensure that any surveillance product has the functionality to pixelate or that appropriate contract is in place for ad hoc pixilation with a third-party company • Ensure appropriate surveillance policies and processes are in place and that any action taken is compliant
• Data Protection Training is mandatory for every member of HSC staff and should be completed at least every 3 years. Data Protection training will reduce the risks to organisations for non-compliance of UK GDPR and should be considered as an additional mitigating measure for the above-mentioned risks.		

Appendix 4 - Examples of Lawful Basis for processing/sharing data and Special Category data include:

1. Lawful Basis for Processing

Article	Lawful Basis	Example
6.1 (c)	Legal Obligation	[REDACTED]
6.1 (d)	Vital Interest	[REDACTED]
6.1 (e)	Public Task	[REDACTED]

2. Lawful Basis for processing/sharing Special Category Data

Article	Lawful Basis	Example
9.2 (c)	Vital Interest	[REDACTED]
9.2 (h)	Health and Social Care treatment or management of HSC systems	[REDACTED]
9.2 (i)	Public Interest in the area of Public Health, Quality and Safety of Health Care	[REDACTED]