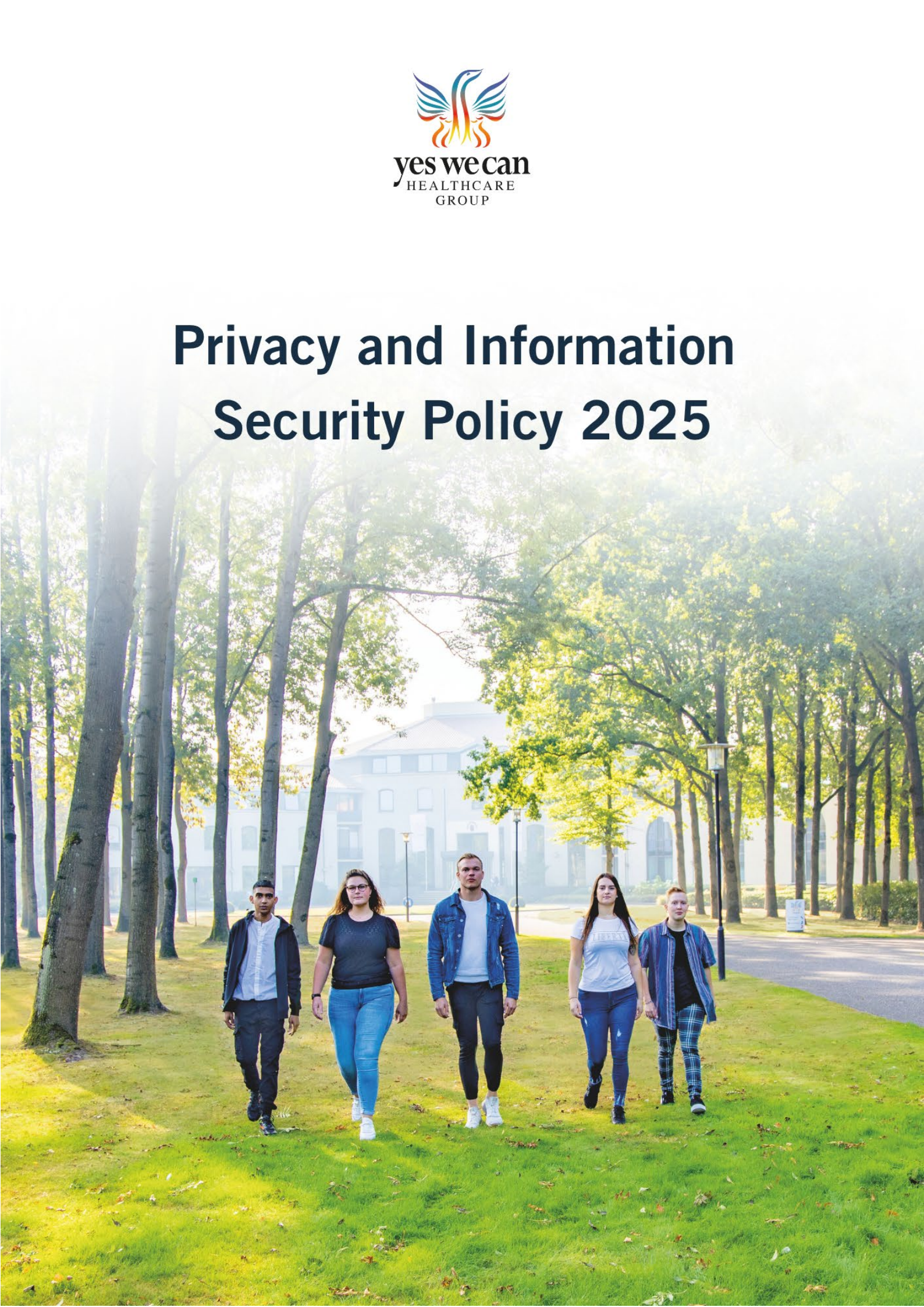
yes we can
HEALTHCARE
GROUP

Privacy and Information Security Policy 2025



Content

1. How does the YWCHG handle privacy and information security?

At the Yes We Can Healthcare Group (YWCHG), we are committed every day to providing a safe and trustworthy environment for our fellows, residents and their families. This commitment extends not only to the care we provide but also to the protection of personal data and the safeguarding of privacy.

We believe it is essential that anyone who comes into contact with one of our organisations – whether through an application, a point of contact or active treatment – can trust that their data is in safe hands. That is why we take our responsibility for handling privacy and data with the utmost seriousness.

The Executive Board of the YWCHG holds overall responsibility for this, supported by the Policy and ICT team. Where necessary, we engage external experts to help identify and assess risks. Every year, we update our risk assessments and revise our policies as needed. This is carried out as part of our annual management review in line with our ISO 9001 and ISO 27001 certifications.

Our principles and procedures are documented in clear and accessible policies, such as our Privacy Regulations and the Quality & Security Policy document. These documents are transparent and available upon request. In addition, our Data Protection Officer oversees compliance with these policies. This data protection approach applies across all parts of the YWCHG, whether data is processed on paper or digitally. In this way, we work together to maintain an organisation where respect, trust, and safety are at the heart of everything we do.

2. Explanation of definitions in this document

At the YWCHG, we believe it is important that everyone understands what we are talking about. That is why we explain below what we mean by the key terms used in this policy.

Personal data – Any information that directly or indirectly relates to an individual. This could include a name, date of birth, telephone number or treatment plan.

Processing of personal data – Everything we do with personal data. This includes collecting, storing, modifying, viewing, sharing, securing or deleting data, both digitally or on paper.

Cookie - A small digital file that is stored on your computer or phone when you visit our website. It ensures the website functions properly and can also remember your preferences.

Staff member - Any colleague involved in the processing of personal data. This usually refers to a therapist, someone in care administration or a member of the secretarial team.

Processor - An external party who processes personal data on behalf of and under the responsibility of the YWCHG. For example, an external research institute or an auditor assessing our quality standards.

Fellow - A young person who is or has been in treatment with us. Parents or guardians may also be considered 'data subjects', as we also process their data. They have the same rights regarding their personal data as fellows do.

Third party - Anyone who is not directly involved in providing care or processing personal data within the YWCHG. For instance, another healthcare provider who receives information.

Consent - When someone gives explicit and informed permission to use their personal data. This must be voluntary, well-informed and specific.

Dutch Data Protection Authority (AP) - The Dutch supervisory authority that monitors whether personal data is handled with due care. This body also has the power to intervene if necessary.

Data breach - When something goes wrong that results in personal data being accidentally exposed or incorrectly processed. Examples include a lost laptop, an email sent to the wrong recipient, or unauthorised access to data.

Security breach - An incident where someone gains unauthorised access to systems or data. This might happen due to hacking or a technical fault.

3. Proper and secure processing of personal data

3.1 How does the YWCHG handle personal data?

At the YWCHG, we only process personal data when:

1. There is a specific, legitimate purpose, and no more data is collected than necessary;

2. We have obtained consent from the fellow/resident or their representative.

In most cases, we process data because:

- It is required to provide effective treatment;
- We are legally obligated to do so;
- It is necessary to prevent serious harm to someone's health;
- It is essential for a public task or for the funding of healthcare services;
- It is in the interest of the Yes We Can Healthcare Group or a third party, and also in the interest of the person whose data is being processed.

Sometimes we process sensitive data such as information about health, religious beliefs, ethnicity, political opinions, sexual orientation or criminal records. This is only done when essential for providing appropriate treatment and support. In these instances, we take extra care to assess whether processing such data is truly necessary for the well-being of the fellow.

3.2 Why do we secure personal data?

The YWCHG secures personal data to protect against loss, inaccuracies, any form of unlawful access or unnecessary storage or processing. In doing so, we carefully consider technical feasibility, costs and the associated risks. This ensures that every decision made about data security is well-informed and justified, providing protection for all individuals involved.

3.3 Who is allowed to process personal data?

Only authorised colleagues are permitted to access and process personal data. We operate with clearly defined access rights, ensuring that each individual only has access to the information necessary for their role. Furthermore, all our staff members – including interns or temporary external workers – have signed a confidentiality agreement.

3.4 Are data processed by (external) processors?

Yes, we occasionally engage external parties to process personal data on our behalf. In these cases, we establish clear terms in a processing agreement. This agreement outlines exactly what may be done with the data, who is responsible for what and how damage is handled. If something goes wrong, the processor is liable, with liability to be assessed by an insurer or court if necessary.

3.5 Who is liable in the event of a data breach?

The YWCHG is ultimately responsible and liable if it becomes evident that we did not take adequate measures to comply with the General Data Protection Regulation (GDPR), including the security requirements outlined in Article 13 of the regulation.

3.6 When can data be shared for scientific research or public health statistics?

Occasionally, our data can contribute to scientific research or public health statistics. This only occurs when it is truly necessary and carried out with due care. The YWCHG makes clear, written agreements with researchers in these instances. These agreements outline the measures taken to safeguard the privacy of fellows and residents.

Data are only shared if the research serves the public interest, cannot be conducted using fully anonymous data, and does not unreasonably infringe on the privacy of the fellow. Data are only shared with explicit consent, unless obtaining consent is not reasonably possible.

3.7 Is there a duty of confidentiality?

At the YWCHG, personal data are only processed by individuals who are legally or contractually bound to maintain confidentiality. When sharing data with third parties, we follow the guidelines set by the Dutch Association of Mental Health and Addiction Care (GGZ). This helps us continue building a safe, trustworthy, and respectful working environment.

3.8 How are personal data stored at the YWCHG?

The YWCHG ensures that personal data are securely stored, in full compliance with applicable laws and regulations, as well as our own high standards for accuracy and reliability. In doing so, we protect the personal data of our fellows, residents, their families and our staff from loss, misuse, or unauthorised access.

3.9 How long are personal data retained?

The YWCHG does not retain personal data longer than necessary. Only when there is real added value – such as for scientific, statistical, or historical research – may data be retained in anonymised form for longer periods. For medical records, the statutory retention period is twenty years, as stipulated in the Medical Treatment Contracts Act (WGBO). Our Register of Data Processing Activities provides a clear overview of how long different types of data are retained. Camera footage, such as from security cameras or observation rooms, is only used for live monitoring and is automatically deleted within a maximum of two weeks.

3.10 What does the YWCHG do in the event of a data breach?

If something goes wrong – for example, if personal data become accessible to unauthorised individuals – it is considered a data breach. At the YWCHG, we take such incidents very seriously. We follow the Data Breach Notification Guidelines issued by the Dutch Data Protection Authority (AP). If the breach potentially has adverse effects on the privacy of those involved, we report it to the AP. If there is a risk to the personal privacy of a fellow, resident, staff member or other party, we will notify the individual concerned. This is part of our commitment to openness, honesty and willingness, brand values that we proudly uphold.

4. Your rights: What can you expect from the YWCHG?

4.1 Is information requested without good reason?

At the YWCHG, we are always transparent about why we request personal data. If we need information from a fellow, resident or another individual, we clearly explain who is requesting the data, what it will be used for, and why it is necessary. We also inform you of your rights and how to exercise them.

The YWCHG is not obliged to inform individuals of a data disclosure if doing so is impossible, would require disproportionate effort, or if the disclosure is required by law or regulation. In such cases, we will clarify that we are legally required to collect or share the data, and under which legislation this obligation falls.

4.2 Can you view or receive a copy of your medical record?

Yes, in most cases you have the right to access or obtain a copy of your medical or care file. You can request this by emailing your treatment coordinator or counsellor, or via the contact form on our website.

- Are you a fellow or were you a legal representative of a child under 16? You may request access or a copy of the medical file via the treatment coordinator or aftercare counsellor.

- Parents of fellows under 16 may also request access to their child's file, provided the fellow gives written, signed consent. During treatment, parents – regardless of the child's age – may be informed of progress, but only with the fellow's consent.

- As a parent or guardian taking part in the parent coaching and counselling programme, you may request access to the data specifically related to your own participation. A fellow cannot access reports about their parents or guardians.

For each request, we verify your identity with a valid identity document and consent form to ensure we are sharing information with the correct person. You will receive the access or copy within four weeks. The YWCHG may (temporarily) deny access if it could be harmful to the health or well-being of the fellow, infringe on another person's privacy or if there are care-related reasons to review the file only in the presence of a practitioner. In cases involving (suspected) child abuse, access to the child's medical record may be denied to parents. Additionally, (divorced) parents do not have access to information about each other.

4.3 Can I access information from the parent programme?

Only parents or guardians who have participated in the parent programme may request access to records specifically concerning themselves. These records only relate to their own participation – not to the fellow, other participants or children. This ensures privacy, transparency and mutual respect.

4.4 What is included in the medical file?

The medical file contains the information necessary to provide appropriate care to the fellow. Not everything that is documented ends up in the file. The following items are not part of the file and are either pseudonymised or deleted within seven years of treatment ending:

- Working documents of practitioners, psychiatrists and nurses;
- Records from supervisory coaches;
- Non-identifiable data from evaluations such as motivation or satisfaction surveys;
- Group session notes where the fellow is not discussed;
- Records from the parent programme.

4.5 Can I amend, supplement or delete my medical file?

At the YWCHG, we believe it's important that fellows have control over their data. As a fellow, you may use the website contact form to request the following:

- Add a personal statement to your file;
- Correct data that is incorrect, incomplete, irrelevant or unlawful;
- Restrict access to specific data for certain individuals;
- Delete data stored under the statutory duty to maintain a file (WGBO).

Please note: Not all data can be deleted. The right to erasure does not apply to administrative or financial records, or anonymised data used for quality improvement or research.

To prevent misuse, each request must include the document number of a valid ID. We will inform you within four weeks whether and how we can comply with your request, along with a clear explanation. The request and our decision will be documented in your file.

We may refuse a deletion request if the law prohibits it, another party (such as a child) has a strong interest in data retention, there is ongoing or expected legal action, or if the file contains information on (suspected) child abuse involving a child under 16 who is legally incapable of consenting.

4.6 Can you object to the processing of your data?

As a fellow, you may object to the processing of your personal data, for example if the data are used for a public task, or for the interests of the YWCHG or a third party. Once we receive your objection, we will assess it carefully. You will be informed within four weeks whether the objection is upheld. If it is, we will immediately cease processing the relevant data.

4.7 Who may act on your behalf in exercising data rights?

If you are twelve years or older and competent, you may decide for yourself how your personal data are handled. In cases involving sensitive data (e.g. suspected child abuse), destruction of the data requires consent from a legally competent youth aged 16 or older.

If you are over 18 but unable to make your own decisions (incompetent), the law designates a representative in this order:

1. A court-appointed guardian or mentor;
2. Someone you have authorised in writing;
3. Your partner or spouse;
4. If none of the above, a child, sibling or other close relative.

If no representative is available or capable, the YWCHG will arrange for a legal representative to be appointed, involving the courts if necessary. You will never be left without support.

4.8 Do we report data processing to the Data Protection Authority?

Yes, when legally required, the YWCHG reports the processing of personal data to the Dutch Data Protection Authority. We adhere to all applicable laws and regulations and are always transparent about what we do with your data and why.

4.9 How does the YWCHG use cookies?

The YWCHG's websites use cookies. Some are necessary for the site to function properly and are always placed. Other cookies – for statistics, preferences or marketing – are only used with your consent. Where possible, data are anonymised. A full list of cookies used can be found in our cookie statement at https://www.yeswecanclinics.com/cookie-statement.

4.10 Do you have a complaint about privacy or this policy?

We strive to handle privacy with the utmost care. If you feel we have not done so, or if you have any questions or concerns, we welcome your feedback. You may submit a complaint via dataprotectionofficer@yeswecangroup.com. Together, we aim to continue learning, improving and restoring trust where needed.

5. Validity of the YWCHG privacy regulations

These privacy regulations take effect on 1 January 2025 and are accessible to everyone via the websites of the Yes We Can Healthcare Group.

For any questions, please contact: dataprotectionofficer@yeswecangroup.com.