OnCall Health Inc.
Privacy Policy (US)

Privacy Policy

OnCall Health allows health care providers to enhance their service with secure video consultations, and patients to consult health care providers from the privacy and convenience of the location they choose. This means personal information and personal health information is collected by OnCall Health. This information is highly sensitive and protected by the Health Insurance Portability and Accountability Act (HIPAA) and all equivalent personal health information protection legislation throughout the United States. OnCall Health is committed to safeguard it at the corresponding level. This Policy describes the physical, technological and administrative measures we implement to safeguard personal and personal health information. We comply with privacy law and we honour the trust of our users by taking every necessary measure to pro-tect personal and personal health information.

By law, personal information is information that relates to an identifiable individual, to the exclusion of business contact information (name, title, work address, work phone number or work email address). Personal health information includes information that relates to an identifiable individual's health, physical or mental, health history including family, or medical treatment.

If we update this Privacy Policy, we will notify you.
Read on to learn more, and if you have questions, feel free to reach our Designated Privacy Contact, Chief Privacy and Security Officer, Nicholas Chepesiuk nicholas@oncallhealth.us,

Our commitment

OnCall Health will never collect, use or disclose personal or personal health information without consent of the individual it relates to.

OnCall Health safeguards personal and personal health information on the basis of risk assessments and industry standards regarding physical security, technological security and administrative policies and processes, as explained further below.

OnCall Health complies with all applicable personal health information legislation where it operates.

What we collect

<u>From health care providers:</u>
We collect name, business contact information, specialization, and college registration number (if applicable).

<u>From patients:</u>
When consulting their own health care provider registered with OnCall Health, we collect:

• Name (or initials) and email of the patient

• Date and time of the appointment
• Any written instructions by the provider added to the "notes for patient" after the appointment,
• Files attached by the provider or patient during or after the appointment inside the platform, usually as PDF or word documents.
• In some cases, results of interactive forms and assessments that are assigned and completed through the system.

How we protect it
OnCall Health protects personal and personal health information through integrated physical, technological and administrative safeguards:

<u>Physical safeguards:</u>
OnCall Health premises are divided into secure areas where electronic equipment and personal and personal health information cannot be accessed without authorization.

Access is controlled by a code and monitored in a manner that keeps all personal and personal health information secure from unauthorized access.

OnCall Health technological equipment does not include portables that leave the premises.
All necessary backups are safely locked.

OnCall Health does not keep personal or personal health information on paper.
Technological safeguards:

OnCall Health stores all personal and personal health information in Northern Virginia, with Amazon Web Services Secure Cloud (AWS). AWS is certified as compliant with ISO Standard 27018 Code of Practice for personal identifiable information (PII) protection in public clouds acting as PII processors. In addition to the independent certification process under ISO 27018, the Standard also includes the right to audit AWS for compliance.

The secure video and/or text consultation is encrypted with the AES cipher using 256-bit keys. Here are the details on our encryption:

• The basic voice, video, and text traffic are converted into cipher, a form which cannot be understood by anyone except authorized parties.
• The conversion is done with random keys that change from the beginning to the end of the conversation to make it even more secure.
• The keys last a short period of time and are neither stored nor persistent anywhere.
OnCall Health destroys or anonymizes all personal and personal health information when it is no longer necessary to deliver service.
OnCall Health employees can only gain technological access to personal information or personal health information collected by OnCall Health:
• With a robust password, based on required elements.
• Upon authorization, granted strictly on a need-to-know basis, defined according to job requirements.

Access is monitored through technological audit trails. Audit trails are regularly reviewed to ensure compliance.

Administrative measures:
OnCall Health has appointed a Designated Privacy Contact, mentioned above, who acts as Chief Privacy and Security Officer (CPSO) responsible for information system monitoring and information security policy and procedure management.
The CPSO is responsible for compliance with OnCall Health's privacy programme including,
• Undertaking threat and risk assessments on a regular basis and as systems are approved.
• Adopting policies and procedures on the basis of threat and risk assessments to mitigate all identified risks, updated as necessary.

OnCall Health users may access their personal information by accessing their account and, should they require assistance, by contacting our CPSO.

OnCall Health closes accounts immediately upon request and destroys or anonymizes all personal information.

OnCall Health completes background checks on all employees before starting employment. As soon as employment starts, OnCall Health trains, supports and supervises all employees on its Privacy Policy and procedures.

Contractors are held to the same high level of protection of personal and personal health information as OnCall Health through contractual agreements, including audits, based on OnCall Health Privacy Policy and procedures.

OnCall Health senior management receives regular reports on privacy compliance and, in turn, reports to the Board for oversight.

OnCall Health is regularly audited by a third party to ensure we are meeting our privacy obligations. This is part of a process for OnCall Health to reassess all policies and procedures on an ongoing basis to ensure that legal requirements are met and personal and personal health information is highly secure.

How we use it
OnCall Heath will never use personal or personal health information for other purposes than why it is provided with consent and necessary to deliver service.

OnCall Health will never rent or sell the personal information or personal health information it collects.

OnCall Health will never disclose personal or personal health information, except as required by law and upon demonstrated lawful authority.

Should OnCall Health conduct market or product research, it would never use personal nor personal health information; rather, it would fully anonymize information which means to render it unlikely to be traced back to an individual.

Should OnCall Health offer users the opportunity to receive relevant information on products or services, or promotions, OnCall Health will seek explicit consent to exercise that option.

Breach response

Experience tells us that there is no total guarantee against data breaches. Damage can be mitigated, however, and OnCall Health has taken all reasonable measures to prevent a breach, as described above.
In the event of a breach, OnCall Health would immediately mitigate its impact by:
• Notifying users at the first reasonable opportunity, namely as soon as we identify the breach,
• Applying remedial measures immediately.

Ensuring patients' meaningful consent

To ensure OnCall Health patients' meaningful consent, OnCall Health provides relevant information in this Privacy Policy, as well as through the availability of our Designated Privacy Contact, nicholas@oncallhealth.sq and subjects use of OnCall Health secure video consultation to the following patient consent form.

To proceed with registration for OnCall Health secure video consultations, a patient must complete this consent form.

OnCall Health Secure Consultation
Patient Consent Form

I agree to OnCall Health secure video or text consultation with a health care provider on the basis of the following information:
OnCall Health will collect my name, the name and contact information of the health care provider, including specialization, as well as the time of appointment.
OnCall Health consultation is occurring on a secure video feed, safeguarded as described in the OnCall Health Privacy Policy.
OnCall Health does not use my personal or personal health information without my consent except as necessary to provide its service.
OnCall will never rent or sell my personal and personal health information.
OnCall will never disclose my personal information except as required by law and upon demonstration of lawful authority.
OnCall will close my account immediately upon request and destroy or anonymize all personal information.