Philips Secure Data Transfer

Terms of Service

Revised: May 10 th, 2012

Thank you for using Philips Secure Data Transfer. These terms of service (the "**Terms**") govern your access to and use of Philips Secure Data Transfer websites and services (the "**Services**"), so please carefully read them before using the Services.

By using the Services you agree to be bound by these Terms. If you are using the Services on behalf of an organization, as an authorized representative of that organization, you are agreeing to these Terms for that organization. In that case, "you" and "your" will refer to that organization. You may use the Services only in compliance with these Terms. You may use the Services only if you have the power to form a contract with Philips and are not barred under any applicable laws from doing so. The Services may continue to change over time as we refine and add more features. We may stop, suspend, or modify the Services at any time without prior notice to you.

Your Content refers to the information that you wish to transfer using our Services.

All recipients of your Content must be registered users of these Services and must agree to these Terms.

Under these Terms, Philips may be referred to as "Philips" or "we" or "our".

Your Content & Your Privacy

By using these Services, you warrant that (i) the transfer of your Content to the recipient is in accordance with the terms, conditions and limitations of liability set out in an existing contract or agreement with that recipient; or, (ii) there is no existing contract or agreement with the recipient, and you are freely providing the Content to the recipient, without limitations or terms or conditions to its use.

By using these Services, you warrant that you are in compliance with all applicable laws and regulations including but not limited to Privacy, Data Protection, Export Control and Copyright law.

By using these Services, you grant us the permission to inspect your Content for auditing and you understand that Philips may also remove any Content from our Services at our discretion. Your permission also permits us to make design choices to technically administer our Services, for example, how we redundantly backup data to keep it safe. You give us the permissions we need to do those things solely to provide and improve the Services. This permission also extends to trusted third parties we work with to provide the Services.

Your Content will be encrypted during transmission and storage. Your Content will be deleted after a specific period of time not exceeding 5 days. We do not take any steps to ascertain that recipients are

your intended recipients of your Content. You retain full responsibility for mistaken identities or names of recipients.

Aside from the rare exceptions we identify in our Privacy Notice, we won't share your Content with anyone other than the named recipients, including law enforcement, for any purpose unless you direct us to. How we collect and use your information generally is also explained in our Privacy Notice.

You are solely responsible for your conduct, your Content, and your communications with others while using the Services. For example, it's your responsibility to ensure that you have the rights or permission needed to transfer your Content to the recipients and comply with these Terms.

We may choose to review Content for compliance with our service guidelines, but you acknowledge that Philips has no obligation to monitor any information on the Services. We are not responsible for the accuracy, completeness, appropriateness, or legality of files, user posts, or any other information you may be able to access using the Services.

Your Responsibilities

The Content that you transfer using the Services may be protected by intellectual property rights of others as well as applicable laws and regulations. You agree that you cannot copy, upload, download, or share files unless you have the right to do so. You, not Philips, will be fully responsible and liable for what you copy, share, upload, download or otherwise use while using the Services. You must not upload spyware or any other malicious software to the Service.

If your contact information or other information related to your account changes, you must notify us promptly and keep your information current. The Services are not intended for use by you if you are under 13 years of age. By agreeing to these Terms, you are representing to us that you are over 13.

Account Security

You are responsible for safeguarding the password that you use to access the Services and you agree not to disclose your password to any third party. You are responsible for any activity using your account, whether or not you authorized that activity.

Acceptable Use Policy

You will not, and will not attempt to, misuse the Services, and will use the Services only in a manner consistent with the Philips Secure Data Transfer Acceptable Use Policy.

Intellectual Property

Philips respects others' intellectual property rights. You agree that you will not knowingly or willfully violate any copyright, patent, trademark or other intellectual property right and you agree that you will not misappropriate any trade secret. We reserve the right to delete or disable Content alleged to be infringing and to terminate repeat infringer's use of the Services.

Termination

We reserve the right to suspend or end the Services at any time, with or without cause, and with or without notice. For example, we may suspend or terminate your use if you are not complying with these Terms, or use the Services in any way that would cause us legal liability or disrupt others' use of the Services. If we suspend or terminate your use, we will try to let you know in advance and help you retrieve data, though there may be some cases (for example, repeatedly or flagrantly violating these Terms, a court order, or danger to other users) where we may suspend immediately at our sole discretion.

Philips Secure Data Transfer is Available "AS-IS"

THE SERVICES AND SOFTWARE ARE PROVIDED "AS IS", AT YOUR OWN RISK, WITHOUT EXPRESS OR IMPLIED WARRANTY OR CONDITION OF ANY KIND. WE ALSO DISCLAIM ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT. Philips will have no responsibility for any harm to your computer system, loss or corruption of data, or other harm that results from your access to or use of the Services or Software.

Limitation of Liability

TO THE FULLEST EXTENT PERMITTED BY LAW, IN NO EVENT WILL PHILIPS, ITS AFFILIATES, OFFICERS, EMPLOYEES, AGENTS, SUPPLIERS OR LICENSORS BE LIABLE FOR (A) ANY INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, EXEMPLARY OR CONSEQUENTIAL (INCLUDING LOSS OF USE, DATA, BUSINESS, OR PROFITS) DAMAGES, REGARDLESS OF LEGAL THEORY, WHETHER OR NOT PHILIPS HAS BEEN WARNED OF THE POSSIBILITY OF SUCH DAMAGES, AND EVEN IF A REMEDY FAILS OF ITS ESSENTIAL PURPOSE; (B) AGGREGATE LIABILITY FOR ALL CLAIMS RELATING TO THE SERVICES MORE THAN THE GREATER OF [$20] OR THE AMOUNTS PAID BY YOU TO PHILIPS FOR THE PAST THREE MONTHS OF THE SERVICES IN QUESTION.

Export Restrictions

You agree that your use of the Services shall always be in strict compliance with all applicable export regulations of the United States of America, the European Union, and the United Nations or local regulations.

Modifications

We may revise these Terms from time to time and the most current version will always be posted on our website. We will notify you of a revision that we feel is material (for example via email to the email address associated with your account). Your continued access to or use of the Services after revisions become effective will be conditioned on your agreement to the revised Terms.

Miscellaneous Legal Terms

THESE TERMS AND THE USE OF THE SERVICES AND SOFTWARE WILL BE GOVERNED BY MASSACHUSETTS LAW EXCEPT FOR ITS CONFLICTS OF LAWS PRINCIPLES. ALL CLAIMS ARISING OUT OF OR RELATING TO THESE TERMS OR THE SERVICES OR SOFTWARE MUST BE LITIGATED EXCLUSIVELY IN THE FEDERAL OR STATE COURTS OF BOSTON ,MASSACHUSETTS, AND BOTH PARTIES CONSENT TO VENUE AND PERSONAL JURISDICTION THERE. These Terms constitute the entire and exclusive agreement between you and Philips with respect to the Services, and supersede and replace any other agreements, terms and conditions applicable to the Services. These Terms create no third party beneficiary rights. Philips failure to enforce a provision is not a waiver of its right to do so later. If a provision is found unenforceable the remaining provisions of the Agreement will remain in full effect and an enforceable term will be substituted reflecting our intent as closely as possible. You may not assign any of your rights in these Terms, and any such attempt is void, but Philips may assign its rights to any of its affiliates or subsidiaries, or to any successor in interest of any business associated with the Services. Philips and you are not legal partners or agents; instead, our relationship is that of independent contractors.

Philips Secure Data Transfer Privacy Notice

Philips believes strongly in protecting the privacy of the personally identifiable information you share with us. We also believe it is important to inform you about how we will use your personal data, and to give you choices about how those data will be used. Therefore, we encourage you to read this Privacy Notice carefully.

This Privacy Notice provides our policies and procedures for collecting, using, and disclosing your information. Users can access the Philips Secure Data Transfer service (the "Service") through our website https://www.sdt.philips.com/ A "Device" is any computer used to access the Secure Data Transfer Service, including without limitation a desktop, laptop, mobile phone, tablet, or other consumer electronic device. This Privacy Notice governs your access of the Secure Data Transfer Service, regardless of how you access it, and by using our Services you consent to the collection, transfer, processing, storage, disclosure and other uses described in this Privacy Notice. All of the different forms of data, content, and information described below are collectively referred to as "information."

1. The Information We Collect and Store

We may collect and store the following information when running the Secure Data Transfer Service:

Profile information. When you register an account, we collect some personal information, such as your name, e-mail address, business phone numbers and business affiliation. You may also provide us with your contacts' email addresses when sharing Content with them.

Files. We collect and store the files you upload, download, or access with the Secure Data Transfer Service ("Files") only for a limited period of time as specified in the Terms.

Log Data. When you use the Service, we automatically record information from your Device, its software, and your activity using the Services. This may include the Device's Internet Protocol ("IP") address, , and other interactions with the Service.

2. How We Use Personal Information

Personal Information: In the course of using the Service, we may collect personal information that can be used to contact or identify you ("Personal Information"). Personal Information is or may be used: (i) to provide and improve our Service, (ii) to administer your use of the Service.

Analytics: We also collect some information (ourselves or using third party services), which can sometimes be correlated with Personal Information. We use this information for the above purposes and to monitor and analyze use of the Service, for the Service's technical administration, to increase our Service's functionality and user-friendliness, and to verify users have the authorization needed for the Service to process their requests.

3. Information Sharing and Disclosure

Philips Auditing. Philips Privacy professionals or Export Control professionals may inspect your Content, profile, and related activity logs in order to evaluate the service, your Content, or your use and we may also remove any Content from our Services at Philips discretion. The purpose of the auditing is for service continuity, improvement and to maintain compliance with law, regulation, policy and the terms of provision of this service. Auditing is performed by Philips professionals or their contracted professional service providers.

Service Providers, Business Partners and Others. We may use certain trusted third party companies and individuals to help us provide, analyze, and improve the Service (including but not limited to data storage, maintenance services, database management, usage analytics, and improvement of the Service's features). These third parties may have access to your information only for purposes of performing these tasks on our behalf and under obligations similar to those in this Privacy Notice.

Compliance with Laws and Law Enforcement Requests; Protection of Secure Data Transfer's Rights. We may disclose, to parties outside Philips, Content stored in your Secure Data Transfer and information about you that we collect when we have a good faith belief that disclosure is reasonably necessary to (a) comply with a law, regulation or compulsory legal request; (b) protect the safety of any person from death or serious bodily injury; (c) prevent fraud or abuse of Secure Data Transfer or its users; or (d) to protect Philips' property rights. If we provide your Secure Data Transfer files to a law enforcement agency as set forth above, we will remove Secure Data Transfer's encryption from the files before providing them to law enforcement. However, Philips will not decrypt any files that you encrypted prior to storing them on Secure Data Transfer.

Business Transfers. If we are involved in a merger, acquisition, or sale of all or a portion of our assets, your information may be transferred as part of that transaction, but we will notify you (for example, via email and/or a prominent notice on our website) of any change in control or use of your Personal Information or Content, or if either become subject to a different Privacy Notice. We will also notify you of choices you may have regarding the information.

Non-private or Non-Personal Information. We will use your aggregated, de-identified or otherwise non-personal, non-Content information for maintenance and improvement purposes such as generating usage statistics of our Service.

4. Changing or Deleting Your Information

If you are a registered user, you may review, update, correct or delete the personal information provided in your registration or account profile by changing your "account settings." If your personally identifiable information changes, you may update it by making the change on your account settings. If you wish your personal Profile information deleted, you can request deletion via email to sdt@philips.com. This may require additional authentication. In some cases we may retain copies of your information if required by law.

5. Data Retention

We will retain your Profile information for as long as your account is active or as needed to provide you Services. We reserve the right to deactivate your account after an extended period (60 days) of inactivity or in accordance with our Terms and Conditions. Your Profile information will be kept no longer than 60 days after your last use of the service. If you wish to cancel your account or request that we no longer use your information to provide you services, you may delete your account by sending an email request to sdt@philips.com. We may retain and use your Profile and other usage information as necessary to comply with our legal obligations, resolve disputes, and enforce our agreements. Consistent with these requirements, we will try to delete your information quickly upon request. Please note, however, that there might be latency in deleting information from our servers and backed-up or archived versions might exist after deletion.

6. Cookies

When you visit the SDT website, we will place one or more cookies. Cookies are small pieces of data (files) that a web site transfers to a users computer. The web site instructs the web browser you are using to visit the website (e.g., Internet Explorer) to store these cookies on your computer. There are two types of cookies. Session cookies are cookies that will be removed from your computer as soon as you close your web browser. Persistent cookies are cookies that remain on your computer, also after you closed your web browser. We use session cookies for security reasons, e.g. to close your session after a longer period of inactivity and we use persistent cookies to remember your preferences and choices in order to optimize your use of the web site.

You have many choices with regard to the management of cookies on your computer. All major browsers allow you to block or delete cookies from your system. To learn more about your ability to manage cookies, please consult the privacy features in your browser.

7. Security

The security of your information is important to us. When you enter personal information on our forms, we encrypt the transmission of that information using secure socket layer technology (SSL).

We follow generally accepted standards to protect and encrypt the information submitted to us, both during transmission and once we receive it. No method of electronic transmission or storage is 100% secure, however. Therefore, we cannot guarantee its absolute security. If you have any questions about security on our service, you can view our Security Overview Page or contact us at sdt@philips.com.

8. Our Policy Toward Children

Our Services are not directed to persons under 13. We do not knowingly collect personally identifiable information from children under 13. If a parent or guardian becomes aware that his or her child has provided us with personal information without their consent, he or she should contact us at philips_privacy_office@philips.com. If we become aware that a child under 13 has provided us with personal information, we will take steps to delete such information from our files.

9. Contacting Us

If you have any questions about this Privacy Notice, please contact us at philips_privacy_office@philips.com.

10. Changes to our Privacy Notice

This Privacy Notice may change from time to time. If we make a change to this privacy notice that we believe materially reduces your rights, we will provide you with direct notification (for example, by email). And we may provide notice of changes in other circumstances as well. By continuing to use the Service after those changes become effective, you agree to be bound by the revised Privacy Notice.

Security Overview

We provide this overview so that you can better understand the security measures we've put in place to protect the information that you store using Secure Data Transfer.

Secure Storage

We encrypt the files that you store on Secure Data Transfer using the AES-256 standard. Encryption for storage is applied after files are uploaded, and we manage the encryption keys.

Secure Data Transfer uses Philips data centers for data storage. Philips stores data over several large-scale data centers.

Secure Transfers

Your files are sent between Secure Data Transfer's device clients and our servers over a secure channel using 256-bit SSL (Secure Sockets Layer) encryption.

Your Content is Not Backed Up

Philips will **not** keep redundant backups of your Content over multiple locations to prevent the remote possibility of data loss.

Privacy

A copy of the Philips Privacy Rules for Customer, Supplier, and Business Partner Data can be found at: http://www.philips.com/shared/assets/Investor_relations/pdf/businessprinciples/PhilipsPrivacyRulesCSBData.pdf .

Philips employees or trusted third parties, in their typical role of managing the services, are prohibited from viewing the content of files you store in your Secure Data Transfer account, and are only permitted to view file metadata (e.g., file names and locations). Like most online services, we have a small number of employees and trusted third parties who must be able to access user data for the reasons stated in our privacy notice (e.g., when legally required to do so or when auditing Content). But that's the rare exception, not the rule. We have strict policy and technical access controls that prohibit employee access except in these rare circumstances. In addition, we employ a number of physical and electronic security measures to protect user information from unauthorized access.

Compliance with Laws and Law Enforcement

As set forth in our Philips Privacy Rules, and in compliance with European Union Member state, United States, and other national laws, Philips cooperates with law enforcement when it receives valid legal process, which may require Philips to provide the contents of your private Secure Data Transfer. In these cases, Philips will remove Secure Data Transfer's encryption from the files before providing your Content to law enforcement.

How to Add Your Own Layer of Encryption to Secure Data Transfer

Secure Data Transfer applies encryption to your files after they have been uploaded, and we manage the encryption keys. Users who wish to manage their own encryption keys can apply encryption before placing files in their Secure Data Transfer. Doing so will also make it impossible for us to recover your data if you lose your encryption key.

I think I've found a security vulnerability. Where do I report security concerns?

We take a number of measures to ensure that the data you store on Secure Data Transfer is safe and secure. While we're very confident in our technology, our processes and our people, we recognize that no system can guarantee data security with 100% certainty. For that reason, we will continue to innovate to make sure that our security measures are state of the art, and we will investigate any and all reported security issues concerning Secure Data Transfer's services or software. For a direct line to our security experts, report security issues to sdt@philips.com.

Secure Data Transfer Acceptable Use Policy

Philips Secure Data Transfer is used by many people, and we are proud of the trust placed in us. In exchange, we trust you to use our Services responsibly.

You agree not to misuse Secure Data Transfer. For example, you must not, and must not attempt to, use the Services to do the following things.

- probe, scan, or test the vulnerability of any system or network;
- breach or otherwise circumvent any security or authentication measures;
- access, tamper with, or use non-public areas of the Service, shared areas of the Service you have not been invited to, Secure Data Transfer (or our service providers') computer systems;
- interfere with or disrupt any user, host, or network, for example by sending a virus, overloading, flooding, spamming, or mail-bombing any part of the Services;
- plant malware or otherwise use the Services to distribute malware;
- access or search the Services by any means other than our publicly supported interfaces (for example, "scraping");
- send unsolicited communications, promotions or advertisements, or spam;
- send altered, deceptive or false source-identifying information, including "spoofing" or "phishing";
- publish anything that is fraudulent, misleading, or infringes another's rights;
- promote or advertise products or services other than your own without appropriate authorization;
- impersonate or misrepresent your affiliation with any person or entity;
- publish or share materials that are unlawfully pornographic or indecent, or that advocate bigotry, religious, racial or ethnic hatred;
- violate the law in any way, or to violate the privacy of others, or to defame others.