Privacy Tips for Medi-Spas and Other Wellness Providers

June 27, 2019

The number of medi-spa and other wellness providers, clients, and services have increased dramatically in recent years. Medi-spas and some wellness providers are subject to conventional health privacy requirements when handling their clients' personal information, even if the services that they provide are not traditional health services. Other wellness providers may not be governed by traditional health privacy laws when handling clients' personal information but are still governed by general privacy laws. In short, privacy compliance is an important concern for all medi-spas and other wellness providers.

This article summarizes some of the essential privacy law principles that apply to the health and wellness industry's regulated health professionals (*e.g.*registered massage therapists, nurses, doctors), non-regulated consultants (e.g. aestheticians, laser technologists), and spa and medi-spa owners and operators.

1. Collect the minimum amount of personal information that you need

Privacy laws address the entire life span of personally identifiable information: its collection from clients, its access and use, its disclosure, and its disposal. We encourage all organizations that collect personal information to start by focusing on the very beginning of this cycle: the collection stage.

Organizations should ask themselves the following:

- What types of personal information do I genuinely need to provide each particular service that a client is seeking to a client?
- For each such type of personal information, what volume of information do I need?

By asking these questions, an organization can ensure that it is collecting the minimum type and amount of personal information necessary in order to provide the service. An organization must make this assessment acting reasonably and with the following in mind:

- service goals;

- relevant health history for indications/contraindications for service,
- risk of exposure to infectious diseases,
- consent to service, and
- authorization to contact other health professionals (if relevant).

For example, if a client is seeking a facial, then it may be important for health and safety reasons for the medi-spa to learn about the client's allergies and past and current skin conditions. However, there may be no such justification for asking for a complete health history.

From this perspective, organizations may wish to think carefully about whether they should be collecting the same personal information from all of their clients, regardless of which service each client is receiving. Drawing on the example above, it may be that the information that is necessary for the medi-spa to obtain from the client receiving a facial is different from the information that the medi-spa needs to collect from a client seeking a massage. It is better for the medi-spa to elicit different, and service-specific, information from each client, using different intake forms, than to use a generic, and very expansive, intake form for all clients, regardless of which services they are receiving.

The need to collect personal information will be determined not only by the specific services being provided to a client, but also by the legal obligations governing the individual providing those services. Regulated health professions are subject to record-keeping requirements under their profession-specific acts and regulations; for example, registered massage therapists must comply with the provisions of the General Regulation made under the Massage Therapy Act, 1991 and with applicable College of Massage Therapy guidelines, policies, and standards of practice. In a similar vein, non-regulated consultants are subject to record-keeping obligations under the Personal Service Settings Regulation of the *Health Protection and Promotion Act*.

2. Use the personal information that you collect appropriately

This ties into the next stage of the information life cycle: appropriate use. When an organization collects personal information from its clients, it does so for identified purposes, and must use the information for those same purposes, or for purposes consistent with them. To go beyond these permitted uses, the organization must first obtain consent from the client.

Organizations should ask themselves the following:

- When I collected this personal information from the client, what was the purpose for which I collected it, as understood by the client?
- What is the purpose for which I seek to use the information now?
- Are these two purposes the same? Or, is the new purpose consistent with the purpose identified at the time of collection?

Once the medi-spa collects information about the client's ongoing skin problems, it can use that information only for the purpose of ensuring the client's wellness when receiving facial services. It cannot use that information for unrelated purposes, such as trying to sell skin care products, unless it first gets the client's consent.

3. Store and handle the personal information securely

We are all accustomed to seeing doctors' offices use safeguards when managing personal information – for instance, storing paper charts in secure areas, requiring users to log in before accessing electronic health records, and examining patients behind closed doors. Medi-spas and their staff are encouraged to think about how to appropriately safeguard the personal information that they acquire in the course of performing their work.

Often, a helpful way to think about information security is to identify the different "points of access" to personal information in the organization – where and how information may be accessed in the course of a workday – and then to build protections around those points of access. These protections may take various forms, and often are divided into the categories of administrative, physical, and technical safeguards. Which specific safeguards are most appropriate will vary across organizations. However, here are some examples of safeguards that may be relevant:

- Educating staff about how to handle confidential client information appropriately,
- Ensuring that paper records are stored in closed cabinets that are locked when appropriate,
- Not leaving paper or electronic information visible to others,
- Backing up electronic records,
- Running software and operating systems updates regularly, and
- Ensuring that staff have access only to the information they need to carry out their work.

This last recommendation is often referred to as "role-based access". Organizations are encouraged to identify the specific personal information to which different staff members need access to do their work. It may be, for example, that an aesthetician only needs access to their own clients' records, and not to those of others. A receptionist, meanwhile, may only need access to appointment lists, but not to records containing personal health information. A manager may need access to everything. A privacy-minded approach would take into account these considerations, and grant the various staff members access to personal information accordingly.

Additionally, organizations are urged to consider the circumstances in which access to personal information should be "cut off," either permanently or temporarily. If an employee goes on leave, for example, there is likely to be no work-related reason why they would need continued access to any client records. It would therefore be appropriate for their access to be suspended until their return to work. Similarly, if an employee leaves the organization, their access should be terminated promptly upon their departure.

Of note, an organization may be required by law to maintain records pertaining to a former employee's work, even after the employee has left the organization. This is because a regulated health professional, such as a registered massage therapist, is legally obligated to maintain clinical documents for each client for a specified time period after that client relationship ends. As a practical matter, this generally means that the organization itself owns the record and maintains it, but the professional continues to have access to the record if needed (for instance, in the event of a lawsuit or regulatory college investigation).

4. Disclose the personal information appropriately

Wellness organizations are also encouraged to think about how they disclose, or share with others, their clients' personal information. In general, personal information should only be disclosed to someone else with the consent of the person to whom the information pertains, or with some legal authority or permission.

Consent is often used to allow personal information to be shared for marketing or similar purposes; however, it can pose its challenges. To be legally valid, a client's consent to disclose information must be informed – the client must understand, for example, what specific information the medi-spa proposes to disclose, and for what purpose. A consent form cannot simply ask a client to agree to something very broad and imprecise, such as, "Do you permit us to use your information for our business purposes?" Additionally, the medi-spa is only permitted to disclose the personal information in the manner contemplated by the consent: it cannot disclose more or different information, or disclose it for a different purpose.

For example, if a client receiving a medi-spa service agrees to have her name and a testimonial about the service posted on the medi-spa's website, then she is providing her consent to have that information disclosed on the website, and the medi-spa is permitted to post it. However, if her consent only addresses the posting of the information on the medi-spa's website, then that is the only place it may be posted. The medi-spa could not also post the testimonial on its social media profiles.

Similarly, if a valid court order is issued, requiring that a medi-spa provide a particular piece of personal information to the police, then the medi-spa is permitted – and in fact required – to disclose that particular information to the police, without obtaining consent from the client whose information is being disclosed. In this situation, the medi-spa should be careful to provide only the information demanded by the court order, and not any additional information. It would also be prudent to document what information is being disclosed, on what date, and to whom, and to retain a copy of the court order.

In the absence of consent or some legal permission or requirement, however, personal information should not be disclosed, and in service-oriented settings like medi-spas, this can be challenging to put into practice. For example, what if a man who is unknown to the medi-spa staff walks in and says he would like to know if his girlfriend receives massages or other services there, because he would like to buy her a gift certificate to the medi-spa? The service-minded response would be to assist him by checking whether the woman he identifies as his girlfriend is indeed a client, and likely even telling him what kinds of services she receives there. What if the man says he would like to mail her a gift certificate and wants to know her street address? Again, the service-minded response would be to provide it to him.

However, as a matter of privacy law, the medi-spa should not be sharing that information with him, because it is personal information that it does not have the client's consent to disclose, and does not have any other legal permission or requirement to disclose. The appropriate response, therefore, would be to explain that the medi-spa is not permitted to provide personal information about its clients, or even to confirm that a particular person is its client.

5. Dispose of the personal information securely

The last stage in the information life cycle is often the easiest to ignore: information disposal. Personal information should be disposed of in a way that will maintain its confidentiality and make reconstruction and re-identification impossible. This means that paper-based personal information should not be recycled, for instance, or even placed in the garbage. Instead, it should be shredded securely. In a similar vein, electronic personal information should be deleted from computers, and any portable media housing personal information should be securely destroyed, not merely thrown in the garbage.

Conclusion

As the number of wellness providers and clients continues to grow, so too will the range and complexity of potential privacy issues arising in the wellness industry. This article aims to give wellness organizations a roadmap to those issues, as they may affect regulated health professionals, non-regulated consultants, and spa and medi-spa operators and owners.

By

Lydia Wakulowsky, Ira Parghi

Expertise

Health Care & Life Sciences, Technology
