Guidance on Gating Mechanisms for Healthcare Professional Targeted Digital Assets

Date: March 2023

Gating Mechanisms for HCP Targeted Digital Assets

Introduction

Through proactive monitoring activities, Health Canada and the PAAB continue to note instances in which healthcare professional (HCP) targeted digital assets (e.g., websites, web apps, and so on) employ gating mechanisms that do not sufficiently restrict access to the primary intended audience. This can cause those digital assets to contravene the Food and Drugs Act, the Food and Drug Regulations, and/or the Controlled Drugs and Substances Act.

Table of Contents

A. Background

The pharmaceutical industry has increasingly leveraged the web to expand accessibility, distribution, and dissemination of healthcare product-related communication assets. It is important to use this effective medium in a manner that adheres to applicable regulations. It is particularly important to consider that the federal laws and regulations which apply to drug promotion in print formats also apply to drug advertising on the web. The following regulations are particularly relevant to the guidance provided herein.

Which communication assets are subject to "advertising" regulations?

> Section 2 of the Food and Drugs Act defines advertising as:
>
> "Any representation by any means whatever for the purpose of promoting directly or indirectly the sale or disposal of any food, drug, cosmetic or

Narcotics and controlled drugs (consumer advertising prohibition)

> Section 70 of the Narcotic Control Regulations and Section G.01.007 of the Food and Drugs Regulations prohibit any advertising from being accessible to the general public for federally scheduled narcotic drugs and controlled drugs respectively.

Rx drugs (consumer advertising restriction)

> The Food and Drug Regulations Section C.01.044 imposes the following restriction on prescription drug advertising accessible to the general public:
>
> *"Where a person advertises to the general public a Schedule F Drug (prescription drugs), the person shall not make any representation other than with respect to the brand name, proper name, common name, price and quantity of the drug."*

Non-Rx healthcare products (consumer advertising restriction)

> The Food and Drugs Act, Section 3(1) imposes the following restriction on non-prescription healthcare product advertising accessible to the general public:
>
> *"No person shall advertise any food, drug, cosmetic or device to the general public as a treatment, preventative or cure for any of the diseases, disorders or abnormal physical states referred to in Schedule A." [See exemption]*

Healthcare professional (HCP) targeted advertising is not subject to the above restrictions and prohibitions provided effective mechanisms are in place to prevent non-HCPs (i.e., "secondary audiences") from accessing the content. Therefore, gates (or "gating mechanisms" or "gating strategies") are employed by Market Authorization Holders (MAHs), their communication agencies, and their suppliers to prevent secondary audiences from accessing digital environments containing HCP advertising. The way in which these gates are implemented impacts their effectiveness. This guidance document has therefore been created to outline best practices when implementing gating mechanisms to help promote adherence with applicable laws. It is the responsibility of all advertisers to ensure that health product advertisements

comply with the requirements of the Food and Drugs Act, its Regulations, and the Controlled Drugs and Substances Act.

It is important to note that applicability of these regulations is not limited to MAH-controlled websites. When placing advertising on third party platforms, the MAH must ensure that the third party has a rigorous process in place to validate users, particularly when the advertising would extend beyond that which would be acceptable in the consumer realm. Note that where the third party's membership/client list would reasonably be expected to be comprised mostly of HCPs, validation against that membership/client list would likely suffice (e.g., **paid subscribers** to a medical journal).

B. Scope

This document is applicable to any digital environment containing MAH-controlled/influenced HCP-targeted communication assets that are subject to advertising regulations and that exceed what would be permissible in the consumer realm.

The therapeutic use(s) of prescription healthcare products authorized by Health Canada can be advertised in environments for which the sponsor has restricted the audience to licenced members of the professions of medicine, dentistry, naturopathy, nursing, pharmacy, and related health disciplines and institutions. This restriction does NOT only apply to traditional print media. It applies to all media, including online/digital advertising (e.g., websites and apps).

In addition to influencing which set of regulations are applicable to advertising materials, the breadth of audience that can access an environment also causes some types of content, which would not ordinarily be considered advertising, to become subject to advertising regulations. The principles outlined in this document are therefore not only applicable to advertising, but to any product-related communication emanating from, or under the control, influence, or sponsorship of Market Authorization Holders (MAHs) that can become subject to advertising regulations through broadened distribution or dissemination. Examples include, but are not limited to, Continuing Medical Education (CME) and MAH medical information portals.

C. Purpose and limitations of this guidance document

For any environment containing healthcare professional targeted communications that exceed consumer advertising regulations, the sponsoring MAH is expected to ensure reasonable controls are in place limiting access, distribution, and dissemination to validated members of a healthcare profession. For electronic tools, there are several ways to meet this requirement.

This document outlines various methods PAAB and Health Canada have seen in practice or have anticipated in theory. It also differentiates which of those methods have a high likelihood of effectively preventing non-HCP access, and which are NOT likely to meet this requirement.

However, using a particular method does not, in and of itself, assure compliance with the regulations. **Ultimately, it is the gating outcome that determines alignment with the regulations, specifically, whether the method or strategy effectively screens out secondary audiences.**

Take, for example, a hypothetical MAH that seeks to implement a gating method which validates licence numbers. This sounds like a robust approach, but the implementation details are important. In this hypothetical case, the gating mechanism is comprised of a single field for user entry of the licence number. This field is labeled "Professional licence number". Note that the licence number is the ONLY input collected from the user. The backend programing syncs the professional licence field with several databases listing active licence numbers to any HCP type across all of Canada's provinces and territories. While this mechanism validates that the entered licence number exists (somewhere in Canada), it will not be effective in preventing non-HCPs from accessing the gated environment. There are numerous licence number formats across different provinces/territories and HCP types. Consequently, an entry comprised of a randomly selected sequence of numbers would have a high probability of resulting in successful entry into HCP web environment. This example highlights that it is important, when considering gating mechanisms, to evaluate the implementation details **AND to stress-test the mechanism** once built (with several random field entries).

D. Gating mechanisms and strategies (the good and the bad)

This section outlines several gating mechanisms that have been implemented over the years. It includes a mixture of mechanisms that have succeeded and mechanisms that have failed to limit secondary audiences from entering the HCP environment with a consistent level of effectiveness. An explanation is provided wherever the mechanism was deemed insufficient along with alterations, where possible, that could render the mechanism sufficiently robust.

Once a user is validated and generates credentials of username + password, these would be a sufficiently robust gating mechanism to be used across MAH platforms without the requirement to re-validate.

D.1 In-house manual validation

Generally acceptable mechanism. The MAH may choose to individually vet users via internal processes as users register for a web portal. When done internally and manually, this usually takes the form of a verbal interaction with MAH staff, for example, HCP contact lists generated from drug representative or medical scientific liaison (MSL) interactions in the field. An additional example would be a HCP calling the MAH medical department staff to register for web access to a medical information portal.

Regardless of how manual validation takes place, users must NOT be granted temporary access to the post-gate content during the validation process. They must only be provided access once they are verified to be HCPs. Among other reasons, any non-authorized user could otherwise simply keep generating fake profiles for temporary access whenever desired.

D.2 Third party HCP status validators

Generally acceptable mechanism. A MAH may enlist the services of existing or future third-party vendors who have rigorous processes in place to validate and maintain up to date records of users' HCP status in order to validate entrants into web environments intended for HCPs.

Regardless of how validation takes place, users must NOT be granted temporary access to the post-gate content during the validation process. They must only be provided access once they are verified to be HCPs. Among other reasons, any non-authorized user could otherwise simply keep generating fake profiles for temporary access whenever desired.

D.3 Registration form without cross-validation

Consider a website landing page that contains a basic form with two fields.

Example D.3.i Insufficiently robust gate:

The user is instructed to enter a licence number and some other piece of information.

For example:
Name + licence number
Profession + licence number
Address of employment + licence number

The only form of validation that occurs is a programming rule dictating that an entry must be made in both fields for the form to be considered complete. Any entry in the fields results in successful passage through the gate. If either or both of the fields are left blank, the website server sends the user's browser an error message and the user remains outside of the HCP web environment.

This is not acceptable. Although two paired pieces of information are requested, this mechanism does not verify that the user is an HCP. The user could gain entry of the HCP website by entering "pineapple" both in the name and licence number fields. While this example seems unlikely, the PAAB has initiated several monitoring instances based on this occurrence in the past two years.

Example D.3ii Insufficiently robust gate:

The MAH layers very general rules onto the prior example (D.3.i). While no cross-validation of any sort occurs, backend programing will now result in failed passage through the gate if non-numeric characters are included in the user-entry within the licence number field. Similarly, passage through the gate will fail if the name field entry includes a number.

This is still not acceptable. This mechanism still does not verify that the user is an HCP. While contextually illogical entries like "pineapple" for the licence number field can no longer result in successful passage through the gate, extremely unrealistic licence number entries like "1" or "99999999999999999" would result in successful passage.

Sections D.4 and D.5 below will build on these examples and outline a couple of different ways to likely increase gating effectiveness by a sufficient extent.

D.4. Automated cross-validation of user-level identification data (e.g., username + licence number)

This entails matching at least one piece of broadly known information that reliably identifies an HCP or their place of work (e.g., name, address of practice, email address, telephone #) with at least one piece of information about that HCP that is less likely to be known by others without conducting some sort of search.

An example of the latter piece of information is the HCP licence number. While members of the general public likely have a HCP's name, place of work, work email address, and/or work phone number on their contact list (or in their human memory), they are less likely to have recorded or memorized that HCP's licence number. Additionally, while this information can be found (e.g., on an Rx, on a licensing college website, or through a browser search), the general public is either largely unaware of this fact or not compelled to execute the physical or electronic search.

In this gating mechanism, the website only permits the user to traverse the gate into the HCP environment if a matching combination of a HCP's name and the corresponding licence number are entered.

> This cross-validation method is considered to be based on user-level data because the server hosting the website executes a check across one or more databases to validate that the entered HCP licence number matches the HCP name entered. If there is a match, the user is taken into the HCP web environment. Otherwise, the user is provided an error message and remains outside of the HCP web environment and/or a notification is sent to the MAH to perform manual validation (during which time the user does not have access to the HCP web environment).

This is likely acceptable as it is expected to yield the desired outcome of restricting secondary audiences from accessing the HCP environment. On the other hand, a combination of HCP name with address/telephone/type of practice would likely not sufficiently restrict access to secondary audiences, even with cross-validation of the input fields, as all requested pieces of information are likely to be in the user's contact list (or human memory).

Other examples of form field pairings resulting in robust cross-validation include:

- HCP work email address with licence #
- HCP work phone # with licence #

Examples of form field pairings resulting in insufficiently robust cross-validation include:

- HCP name with province
- HCP name with practice address
- HCP name with practice phone number

D. 5 Automated cross-validation based on an abstraction from user-level data (e.g., expected format/pattern of user-entered HCP licence number)

At a minimum, wherever this gating mechanism is employed, the pre-gate landing page has the following user entry fields:

- Province (e.g., dropdown field)
- Health profession type (e.g., dropdown field)
- Licence (e.g., open alphanumeric field)

Different HCP licensing bodies within different provinces and profession types have different licence number formats and patterns. The gating method described in this section leverages that fact by setting an expected licence ID pattern/format **that is conditional on BOTH the user-selected HCP type and the user-selected province/territory**. Note that the expected licence ID

pattern/format is an abstraction or generalization from the actual registry of individual licence numbers for any particular HCP type in any particular province. Once the expected pattern/format is set for each pairing of HCP type and province, programming logic is implemented on the backend to cross-validate that the user entry into the licence field has the precise pattern/format expected for the corresponding pairing of HCP type and province.

The user successfully enters the site only if BOTH are TRUE:

- The format of the licence field entry matches the format expected for the combination of selected HCP type and province, i.e., correct length + correct composition (when the licence includes one or more letter(s), their position should also be considered).
- The entered licence number is not unrealistic (e.g., 00000, 00001, 99999, -3261). See Guardrail 3 below.

It is critical that all pattern/format attributes of the licence number be incorporated into the expected format. For example, if the licence issued for a particular HCP type + province pairing is comprised solely of numbers, a user entry that includes one or more letters must NOT result in successful passage through the gate, even if the field input has the correct total number of characters. Similarly, if the issued licence includes a letter or it always includes a particular number in a particular location, this must be reflected in the user-entry for successful passage through the gate.

The underlying premise of this mechanism is that the user is **likely** an HCP if the licence field input matches the pattern/format that is expected for the user-selected combination of HCP type and province. Of course, this premise is **only valid if** it is unlikely that the user would gain access to the HCP environment by populating the licence field with random numbers.

This mechanism is likely acceptable if guardrails 1 through 4 are always implemented, and guardrail 5 is implemented where needed based on stress-testing.

Guardrail 1:
No cues or hints!!
No cues/hints are provided regarding the expected format for the licence entry.

> *E.g.: a licence example must not be provided (as this would provide a hint about the required format)*
> *E.g.:* When an incorrect entry is made, no guidance is provided to cue appropriate format (e.g., returning an error state that reads "Licence number must be 6 digits").

Guardrail 2:
Don't format the field in a manner that makes it easier to guess correctly!!
The licence field accepts any combination (of many possible lengths) of alphanumeric keys. Users must be provided all opportunities to unknowingly deviate from the expected format.

> *E.g.: The field must not be locked to allow a maximum of 6 digits if the expected licence format is a 6-digit number.*

Guardrail 3:
Unrealistic patterns = wrong!!
Entries that match the expected licence length and composition for the entered province + HCP type pairing (e.g., 5 numeric keys), fail entry if they are unrealistic. For example, entries like 00000, 00001, 12345, 99999, and so on, should not result in successful gate crossing unless these are actual licence numbers.

Guardrail 4:
Test your gating creation!!
Health Canada is more concerned with gating effectiveness than the selected gating methodology. It is therefore advisable to test the gate robustness. This can be done by ensuring that random licence field entries are much more likely to result in blocked access to the post-gate website content.

Guardrail 5:
Based on testing, consider the need to narrow the range of access-resulting licence field entries.
If random licence field entries frequently result in website access, the gate is strengthened by further narrowing the range of access-resulting licence field entries. For example, this can be accomplished by disqualifying website access for licence field entries that are much lower and/or higher than expected for currently living or practicing members of a given HCP-type + province pairing. This goes beyond disqualification of individual unrealistic numbers/patterns in Guardrail 3. Guardrail 5 likely won't be needed for the vast majority of HCP type + province pairs. However, it is an important approach to consider whenever the gate is readily traversed with random licence field entries.
Some licensing bodies provide the entire updated set of active licence numbers on a spreadsheet that is downloadable from their website. Others may provide a spreadsheet of active licence numbers on request, particularly if individually identifying information (such as names, addresses…) can be excluded.

NOTE: This cross-validation method is not based on user-level data. The server hosting the website simply executes a check that the user-entered licence number follows the expected format/pattern that has been programmed into the conditional logic for the corresponding user-selected province and HCP type pairing.

Note the licence field entry must be cross-checked against BOTH the HCP-type field entry and the province entry. It is not sufficient to only cross-check the licence field entry against one of these other fields UNLESS post-gate entry is limited to only one HCP type or HCPs from a single province. Cross-checking against only these fields results in a weak barrier against random licence field entry.

D.6 User reported status/information

D.6.i Attestations

Indicating an agreement to the "terms of use" (e.g., "I confirm that I am an HCP") **would not meet the requirement** of posing a true barrier to entry from non-HCP audiences.

D.6.ii Social media profiles

Social media profiles such as Facebook or Twitter may allow for the user to identify their profession. However, these platforms **do not verify the accuracy of these user entries**. This is also true of professional social platforms such as LinkedIn. The theoretical possibility that a contact might identify (and perhaps try to rectify) an inaccuracy does not render social profiles a robust mechanism to validate HCP status.

Targeting users with advertising that exceeds consumer regulations based solely on a social profile is not acceptable.

It is important to note, however, that **user membership in a network for which HCP status is robustly & independently validated could be used to validate that the user is a HCP**. In fact, linkages from one HCP web environment can be set to bypass the gate into another HCP web environment (as HCP status has already been confirmed).

D.7 Device or browser tracking

Note that with increased value and attention placed on cyber data privacy, some of the mechanisms listed below are on the decline from the perspective of availability and/or user appetite. Where these mechanisms remain available, they must only be employed following intentional and informed user opt-in.

D.7.i IP-address filter

IP-address filters are occasionally used to verify that a computer is affiliated with an institution (such as a university, hospital, or clinic) that has subscribed to a particular service. While this mechanism could be set up to block users who are not affiliated with that institution from accessing content, it **does not limit access to healthcare professionals**.

For example, a medical journal website has a gating mechanism based on an IP-address filter that identifies universities and hospitals that have subscribed to the journal. Access to the entire journal website is automatically granted to any user on a computer that has an IP-address registered on the website's database. While this does not allow access to the general public, it allows access indiscriminately to any user on those computers (without regard to whether they are healthcare professionals or even in related job functions).

D.7.ii Cookies

While it is possible to use cookies across various websites to track which browsers have successfully crossed a robust HCP gate on a tracked site, this alone does not verify that

all users of the web-browsing device are HCPs. While legitimately crossing the HCP gate should give the user access to all HCP content within that same browser session, it should not, **by default**, provide the browser access to the post-gate sections in later browser sessions. **Cookies alone are not a sufficient barrier**.

Targeting browsers with advertising that exceeds consumer regulations based solely on the browsing history is not acceptable.

Cookies IN COMBINATION WITH user opt-in is a sufficient barrier.
It should be noted, however, that this approach is acceptable with user opt-in. Once the user is validated to be an HCP, it is acceptable and appropriate to employ a mechanism to remember the browser and/or device for direct entry into the same and affiliated websites. Again, this functionality should require the user to opt in (i.e., should require a click rather than occurring automatically in the absence of a click).

D.7.iii Geolocation

Geolocalization, also known as geotracking/geopositioning, is the process of estimating the geographic location of an object (in this context, typically a mobile device). For example, geolocalization can determine which phones are consistently in close proximity to a hospital or clinic. One might surmise that persons in possession of phones that are regularly in close proximity to a hospital for extended periods of time (e.g., 8 hours per weekday) are HCPs. However, **this is not a sufficiently robust mechanism to validate HCP status** as non-HCPs are also often in close proximity to a hospital or clinic for extended periods of time.

Combination of geolocation AND cookies *may* create a sufficient barrier.
While cookies (without opt-in) and geolocation are not generally sufficient on their own, their combination **(particularly for mobile devices)** may create a sufficiently robust barrier for preventing secondary audience access of HCP web environments.

For example, it is very likely that someone who is regularly near a clinic for a substantial segment of each week AND who frequently visits medical websites on their mobile (i.e., personal) device is an HCP.

D.8 Medical knowledge assessment

An MAH website landing page is set up to require the user to answer a medical question in order to gain entry into the HCP segment of a website.

Examples for the question field:

- Enter the maximum dose of drug X
- Enter the three-letter complex that the ST segment connects with the T wave in electrography

The website's server will then compare the entered answer with the answer deemed to be correct. If there is a match, the user gets access to the HCP web environment. Otherwise, the user is provided an error message and remains outside of the HCP web environment.

Medical trivia is **not an effective gating mechanism** as medical knowledge is not limited to HCPs and therefore does not identify HCPs. While medical trivial may be useful as a tool to increase user engagement, it would not be considered a robust gating mechanism.

D.9 Preventing a website from appearing in browser search results

The combination of using a URL that is not easily guessable and taking effective steps to prevent the website from appearing as a browser search result **can be a robust strategy for restricting a web environment to HCPs**.

Examples of **easily guessable** URL:

- www.arbace.ca
- www.arbace.com

Examples of **acceptable** versions:

- www.arbacehcp.ca
- www.arbace-hcp.ca
- www.arbace-info.ca
- www.arbace-studies.ca

This method requires ensuring the MAH's actions were effective in preventing the site from appearing in the first few pages of search results. Insertion of the no-index command on each of the website's pages is generally considered an effective way to block indexing. The MAH should periodically check that the method is producing the expected result. This monitoring should take place on all common browsers. Different browsers can sometimes behave differently when it comes to deindexing websites.

This method also requires that the MAH has a controlled manner to distribute the URL, QR code, or hyperlink to HCPs (e.g., a mailing list or email list of validated HCPs, in-person distribution through drug representatives, distribution at conference booths, and so on).

When this strategy is employed, the URL, QR code, or hyperlink essentially becomes a password that provides access to the HCP environment. Hardware, such as a USB stick that was distributed in a controlled manner, might also be used to automatically launch a digital asset when plugged into a computer.

CAVEAT: If a website had previously been indexed, simply introducing no-index commands on each page will not necessarily immediately remove the site from browser search results. Additional steps that depend on the browser may be required. For example, if a browser continues to index a website in spite of the coded robot commands, the settings in the browser's webmaster tool may need to be changed.

CAVEAT: When blocking indexing as a gating strategy, users cannot be directed to the website through linkage from another non-gated website.

D.10 Access codes distributed in a controlled manner

Access codes for digital assets, that are either gated or whose browser indexing is blocked, can be distributed by MAH representatives in a controlled manner to HCPs. For example, this distribution might take place through sales representatives or MSLs as appropriate (based on the type of content in the digital asset and the applicable principles in the Health Canada policy document "The Distinction Between Advertising and Other Activities"). Recipients of the access codes would be considered validated given the controlled method of distribution.

Exemption to Section 3 of the Food and Drugs Act

Sections A.01.067 and A.01.068 of the F&DR, and Sections 103.2 and 103.3 of the *Natural Health Products Regulations* (NHPR), exempt natural health products (NHPs) and non-prescription drugs from the F&DA's Section 3 general restriction on labelling and advertising of preventative claims for Schedule A diseases. Claims for the prevention of Schedule A diseases may appear in advertising for NHPs and non-prescription drugs provided the claims are consistent with the product's TMA and do not directly or indirectly exceed the scope of the TMA.