

## British Columbia Pharmacy Association

Suite 1530 - 1200 West 73rd Avenue

Vancouver, BC V6P 6G5

Tel: 604 261-2092 Fax: 604 261-2097

info@bcpharmacy.ca www.bcpharmacy.ca



January 12, 2016

Mr. Bob Nakagawa  
Registrar  
College of Pharmacists of British Columbia

Dear Bob:

Re: PPP-74 Bylaw

Pharmacy robbery is a real and frightening problem. The BCPhA Board strongly supports the use of increased security measures to protect registrants<sup>1</sup> and so we were pleased to participate in the Robbery Prevention Working Group when it was constituted in 2013. The Working Group worked hard and in good faith to collaborate on the development of a new security standard that would deal with the harms posed by the rise in drug thefts. Regrettably, the process was flawed, and the result has been confusion, delay, and substantial expense.

In the November edition of ReadLinks, you wrote that the College seeks to follow the model of *Right Touch Regulation* and find the balance between over- and under-regulation, and to be clear and supportive, not overly prescriptive. The Association supports this effort to develop a balanced regulatory framework so that professionalism can flourish and continuously improve.

A *Right Touch Regulation* approach requires collaboration and consultation throughout the process. It means identifying and clearly defining the problem, quantifying the risk and focusing on outcomes that are *responsive* to the problem and actually mitigate the risk. Only through rigorous and comprehensive collaboration with stakeholders can this be accomplished while avoiding unintended consequences.

That's why we're encouraged to see the College reaching out to initiate dialogue about the new draft security bylaw. We look forward to the meeting scheduled for January 26. We consider this a good start to a more productive approach to consultation, including one-on-one meetings at which stakeholders' perspectives can be explored in good faith and be better understood. We believe that by working together we can improve the regulatory framework for the benefit of the public and the profession.

We're pleased to see some suggestion in the proposed bylaw and its policy document (revised PPP-74) of a less prescriptive and more principled approach. That said, we still have substantial concerns about the draft bylaw, which remains less a principle-based document standard than a highly prescriptive rule. By imposing highly detailed operational requirements, the bylaw and policy would prevent registrants from ensuring that their specific security challenges are actually addressed in a manner that is *practical, reasonable and relevant to their own circumstances*. And it runs the risk of putting registrants in conflict with other legal duties they owe under privacy and employment law.

Since we are certain this wasn't the intention, we will set out our concerns with both the process and the result in this document. We do this with a view to facilitating the *Right Touch* approach of i) identifying and defining the problem; ii) quantifying the risk; and iii) focusing on outcomes that are responsive to the problem and mitigate the risk, while avoiding these unintended consequences that we now see.

---

<sup>1</sup> Submission letter to Suzanne Solven from Geraldine Vance dated February 11, 2015

### **i) Identifying and Defining the Problem**

From the beginning, the purpose of the Robbery Prevention Working Group was to deal with the rise in drug thefts. The Terms of Reference are very clear: review current pharmacy security standards for robbery prevention in BC and other jurisdictions; develop bylaws or policy for pharmacy security requirements; report to the Board as applicable.<sup>2</sup>

The *Community Pharmacy Security Standards and Resource Guide*, developed collaboratively and completed in January of this year, explains that the policy was meant to address “potential or actual loss in pharmaceuticals, particularly controlled drugs and precursors [through] robbery, break and enter, drug diversion, theft, drug loss (unexplained or adulterated).”<sup>3</sup> And indeed, these are the issues the Working Group worked on.

That is why we were surprised when the privacy issue was first raised in April 2015. This had never come up before and was not within the Terms of Reference for the Working Group. We are surprised to see this carried over into the bylaw in the definition of “pharmacy security”. Including “protection of confidential patient information” as a “measure to prevent and respond to incidents of robbery, break and enter, forgery, theft, unexplained drug loss or adulterated drugs at a pharmacy” is highly problematic. First, it is simply unrelated to drug theft issues that are meant to be addressed by the notion of pharmacy security. Second, the duty to maintain confidentiality *already exists* in s. 3(2)(n) and the duty to make reasonable security arrangements to protect personal information *already exists* in s.3(2)(o). So the inclusion here is redundant. But it has serious implications for registrants. Adding this concept into “pharmacy security” creates internal inconsistency in the bylaw because now we don’t know whether or not meeting 3(2)(n) and 3(2)(o) will be sufficient to meet the pharmacy security requirements. Are they the same or different?

The simple fact is a drug theft is not the same thing as a privacy breach. The nature of the problem, the scope of the duties and risks and the potential harms are very different. The two issues must be kept separate to ensure that each is properly analyzed. There are different statutory, contractual and ethical duties, and risks, arising in drug thefts and privacy breaches. Conflating the two issues in this way to justify the College’s last-minute, unilateral imposition of the mandatory barriers requirement serves no one. And it is wholly inconsistent with the *Right Touch Regulation* approach.

We strongly recommend removing “protection of confidential patient information” from the definition of pharmacy security. These amendments should not attempt to address informational security issues, which were out of scope of the Working Group, are already highly regulated areas, and for which registrants have already developed policies and procedures which take into account these other regulatory requirements.

### **ii) Quantifying the risk**

The law is clear that bylaws must be reasonable, and that reasonableness is context-specific and highly dependent on the level of evidence to support the need for the bylaw. There is no evidence that PPP-5 was inadequate or needed amending. Indeed, there is a lack of evidence to support the policy decision to make security barriers mandatory across all community pharmacies in the province.

So the College’s insistence on proceeding with this and abandoning the alternatives permitted under PPP-5 is troubling, especially in the context of its deliberate and continuing exclusion of the Working Group from this decision.

Initial Working Group meetings were held on April 9, 2014; June 9, 2014; and Sept 15, 2014. On December 9, 2014, the first draft of PPP-74 and the Resource Guide was issued to members of the Working Group for review. At that time, there was no mention of security barriers. The second round of draft documents, reviewed for the meeting on January 9, 2015, also contained no mention of security barriers. On February 18 and 19, 2015, the Board approved PPP-74 including the security barriers requirement.

---

<sup>2</sup> *Robbery Prevention Working Group Terms of Reference*

<sup>3</sup> *Community Pharmacy Security Standards and Resource Guide* at page 8

The Working Group deliberated in good faith on issues associated with drug theft, and concluded that monitoring technology, together with alarms systems, time lock safes and the procedural requirements in PPP-74 were sufficient to respond to the problem. The Working Group's process was reasonable and those results are practical and proportionate to the risk. Further, and simply as a practical matter, those requirements can actually be implemented within a reasonable time for a reasonable cost.

The same just can't be said of the security barriers issue. Simply put, *no work was done* on this issue. It is not clear what problem the barriers will mitigate that isn't sufficiently mitigated by the other security tools required to be used. No evidence was collected as to the risks of not having barriers, and therefore it is not clear that barriers are necessary or that the barriers mitigate risks better than other methods of controlling access. No competing concerns were considered, such as the costs of barriers and the impact on registrants' operations. Finally, it appears that this section will conflict with telepharmacy operations, with the pre-existing bylaws in respect of personal information protection, and with s. 12 (Operation without a Full Pharmacist). Nothing about this part of the process has a "right touch."

Additionally, mandating that the barriers must "maximize" access prevention is much too high a standard and does not allow for any balancing with business needs including service delivery requirements. Privacy laws and other College bylaws impose a "reasonableness" standard which permits organizations to apply a standard that is "reasonable and appropriate in the circumstances". The requirement to "maximize" access prevention through the use of physical barriers does not account for the use of procedural tools routinely used to protect personal information and maintain security.

In sum, the prescriptiveness of this requirement is inherently unfair. It doesn't take into account differences among pharmacy size, location, risk profiles, staffing levels, operations or a myriad of other issues. Moreover, in situations such as telepharmacy, where the point of operating the telepharmacy is to provide health care to people where there is no full pharmacist available, requiring barriers in the absence of a full pharmacist simply makes no sense. Given the vast differences in the physical layouts of community pharmacies across the province, it is inappropriate – and frankly impossible - to mandate a "one size fits all" requirement.

We are encouraged by the suggestion in the policy document that a locked cabinet might be sufficient to meet the requirement in the bylaw for 'physical barriers' but unless the term is defined in the bylaw itself to include the range of examples provided in the policy, registrants will have no way of determining what is reasonable in their own circumstances. Currently, the vagueness of this requirement leaves inspectors with too much scope for arbitrary decisions as to registrants' compliance. And finally, we suggest that the reference to "confidential patient information" be removed from 11.1(3) because that issue is dealt with in s. 3(2)(o).

Accordingly, we suggest that a definition of physical barriers be added to the bylaw, as follows:

"physical barriers" means an impediment to access and includes a lockable gate, cabinet, case, door, or screen, or grillwork or panel or other similar things.

And we suggest that s. 11.1(3) be amended as follows:

11.1(3) A community pharmacy must use physical barriers that are reasonable and appropriate in the circumstances to prevent access to Schedule I, II and III drugs, narcotics and controlled drugs when no authorized person is present.

And we suggest adding a definition of "authorized person" as:

An "authorized person" is a registrant or a pharmacy assistant;

The corresponding sections in PPP-74 and its resource guide describing "Physical Barriers" should be amended accordingly.

## Other Concerns

In addition to the forgoing, we have some comments on other aspects of the amendments that we are concerned may in their current form result in real confusion among the profession and excessive administrative challenges for the College. First, we suggest that the notification requirements in s. 3(2)(s.1) and 3(2)(s.1)(bb) are overbroad and vague. They seem to require managers to report to the College about *any* instance of non-compliance and the burden will be on the manager to assess whether the issue should be reported.

We have real concerns about the degree of accountability this imposes on managers and the impact on the employment relationships of registrants. Further, this risks establishing an adversarial relationship between employers and employees because the manager is required to act in an essentially regulatory role, to assess and determine whether a particular operational decision is “compliant” with the bylaws. But employees have duties to their employers, including duties of confidence, loyalty and good faith. In the ordinary course, an employee with concerns about an employer’s compliance should raise the issue internally and only where there is a real risk of harm, or a good faith belief that non-compliance is knowing and intentional, would it be appropriate to report.

In addition, the bylaw includes no protection for an employee who makes a good faith report of non-compliance; it mandates whistleblowing on even the most minor or transient matters, but provides no support to the whistleblower. Finally, what if the manager has a reasonable belief that the policy or act is compliant such that no report is required, and the College ultimately determines that there was non-compliance? Will the manager be subject to discipline by the College for the failure to report?

In other words, the employee may be required to choose between avoiding discipline by the College or discipline by the employer. These concerns will be factors that artificially drive up the number of reports that will be made, or, conversely, artificially drives them down.

All of these issues are exacerbated by the “Notification Procedures” in the draft PPP–74, which also suggests that under 3(2)(s.1) “*any*” breach of pharmacy security must be reported, but that managers should also notify owners and directors immediately of a breach and that action should be taken to resolve the issue, which presupposes that the issues may be resolved internally, after which point, obviously, there would be no breach and no need to report. It also refers to “the minimum pharmacy security requirements” but what is minimally required is not explained anywhere. Clearly, 3(2)(s.1) needs to list the kinds of breach to be reported and differentiated from incidents of malfunction.

Again, we suggest that to mandate reporting of *all* breaches, regardless of size, materiality, intention or risk, and in the absence of whistleblower protection, imposes substantial, unfair duties on employees and will harm the employment relationships. Until the implications of a mandatory reporting requirement can be properly assessed by the Working Group, we strongly urge the College to withdraw these sections in their entirety.

At minimum, we suggest that the notification requirements be amended as follows:

3(2)(s.1) after notifying the owners and directors and, if appropriate, police, notify the registrar of a breach of pharmacy security including:

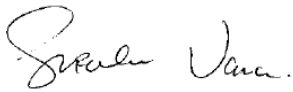
- (i) Robbery or attempted robbery, break and enter and prescription forgeries, and
- (ii) Other forms of an unresolved security breach if after bringing it to the attention of the owner(s) and director(s), it clearly continues to pose a risk of significant harm to the pharmacy or the public;

3(2)(bb) Notify the registrar where the manager’s concern about compliance has been brought to the attention of pharmacy owner(s) or director(s) and the manager has a good faith belief that there is (i) a real risk of significant harm from the suspected non-compliance; or (ii) intentional, deliberate and ongoing non-compliance by the owner(s) and director(s);

Finally, surveillance is inherently privacy-invasive and the requirements for high-resolution cameras puts individual privacy at risk. Cameras collect substantial amounts of personal information of customers and of employees, by recording all the activities within the pharmacy throughout the day. This imposes substantial privacy obligations on the pharmacies to protect this data. Most community pharmacies will already have surveillance cameras and retention policies around this data in compliance with applicable privacy laws, which mandate that personal information be retained *only as long as necessary for the purpose*. Generally, video surveillance information is retained long enough to be retrieved in the event of an incident. These will have already been determined by each pharmacy and are likely to be much shorter than 30 days. Imposing a 30 day requirement is arbitrary and may prove problematic for most registrants, who already have surveillance systems in place. We strongly urge you to do away with the 30 day retention period requirement.

We look forward to further discussions and consultation on these issues as this matter moves ahead.

Sincerely,

A handwritten signature in cursive script, appearing to read "Geraldine Vance".

Geraldine Vance  
CEO, BC Pharmacy Association

CC. Blake Reynolds, Chair, College of Pharmacists of British Columbia