PHIA Privacy Breach Risk Rating Tool

Subsection 19.0.1(2) of the Personal Health Information Act (PHIA) sets out requirements for notifying individuals of a privacy breach when a real risk of significant harm has been created for those individuals. Section 8.7 of the PHIA Regulation includes the relevant factors that *must* be considered when determining whether a real risk of significant harm occurred.

The table below summarizes the risk factors listed in section 8.7 of the regulation, provides examples, includes assessments and suggests *possible* risk ratings for each risk factor. The examples are for illustrative purposes only. It is important to note that trustees and public bodies must make their own assessments of risks given the unique circumstances of privacy breach situations. The table is intended to provide some general guidance to ratings, but is not an exhaustive list.

RISK FACTORS	RISK RATINGS		
	Low	**Medium**	**High**
Nature of personal health information (a) the sensitivity of the personal health information involved; (c) any other factors that are reasonably relevant in the circumstances.	☐ Publicly available personal health information not associated with any other information. The information would not normally be disclosed but would not result in harm. (Ex: a listing of civil servants that have regular or extended health insurance benefits, without associated identifying health plan beneficiary or group numbers)	☐ Personal health information that identifies an individual as a patient of a trustee but does not contain details of diagnosis, treatment or health care provided. (Ex: a paper list of a trustee's patient appointments for one morning is lost. The list contains only the trustee's name, patient names and appointment times. No other information about the patient, their condition or care would be revealed.)	☐ Medical, mental health, psychological, counselling, or PHIN number ☐ Information relates to a vulnerable individual, a youth or senior. (Ex: a patient's mental health record is sent to a third party in the same community)
Scope of the breach (b) the probability that the personal health information could be used to cause significant harm to the individual, having regard for: (ii) the number of persons who actually or potentially accessed the personal health information, (iii) if the identity of the persons who actually or potentially accessed the personal health	☐ Very few affected individuals ☐ Very few people could have accessed/viewed the personal health information	☐ Identified and limited group of affected individuals ☐ Identified and limited group of individuals could have accessed/viewed the personal health information but confirmed full deletion or secure destruction of the information without viewing	☐ Large group or entire scope of group of affected individuals not identified ☐ Large group of individuals or entire scope of group not identified, who could have fully accessed/viewed the personal health information and the information has not been recovered

information is known or unknown, (vi) the length of time since the privacy breach first occurred and the duration of the period in which the personal health information was available to be accessed, used, disclosed, destroyed or altered in contravention of the Act, vii) the amount of personal health information involved (c) any other factors that are reasonably relevant in the circumstances.			
Relationships (b) the probability that the personal health information could be used to cause significant harm to the individual, having regard for: (iii) if the identity of the persons who actually or potentially accessed the personal health information is known or unknown, (iv) any known relationship between any of the persons who actually or potentially accessed the personal health information and the individual to whom the information relates, and the nature of the relationship, (v) if the trustee is reasonably satisfied that any person who actually or potentially accessed the personal health information has destroyed any unauthorized copies of it and has committed to not use or disclose it,	☐ Accidental disclosure to another public body or trustee who reported the breach and confirmed destruction or return of the information	☐ Accidental disclosure to a stranger who reported the breach and confirmed the destruction or return of the information	☐ Used by or disclosed to an individual with some relationship to or knowledge of the affected individual(s), particularly disclosures to ex-partners, family members, neighbours or co-workers ☐Theft by a stranger

(c) any other factors that are reasonably relevant in the circumstances.			
Cause of the breach (b) the probability that the personal health information could be used to cause significant harm to the individual, having regard for: (i) the event that caused the privacy breach to occur, including whether there is evidence of any malicious intent, such as the breach being the result of theft or gaining unauthorized access to a computer system, (c) any other factors that are reasonably relevant in the circumstances.	☐ Technical error that has been resolved	☐ Accidental loss or disclosure	☐ Intentional breach ☐ Theft ☐ Hacking, Ransomware, Phishing ☐ Unauthorized access to paper files ☐ Unauthorized access to a computer system ☐ Cause unknown ☐ Technical error (if not resolved)
Containment efforts (b) the probability that the personal health information could be used to cause significant harm to the individual, having regard for: (v) if the trustee is reasonably satisfied that any person who actually or potentially accessed the personal health information has destroyed any unauthorized copies of it and has committed to not use or disclose it, (vi) the length of time since the privacy breach first occurred and the duration of the period in which the personal health information was available to be accessed, used, disclosed, destroyed or altered in contravention of the Act, (viii) if the personal health information has been recovered,	☐ Data was adequately encrypted ☐ Portable storage device/ laptop was remotely erased and there is evidence that the device/laptop was not accessed prior to erasing ☐ Hard copy files or device were recovered almost immediately and all files appear intact and/or unread	☐ Portable storage device/laptop was remotely erased within hours of loss but there is no evidence to confirm that the device was not accessed prior to erasing ☐ Hard copy files or device/laptop were recovered but sufficient time passed between the loss and recovery that the data could have been accessed	☐ Data was not encrypted ☐ Laptop access was not user ID/password protected ☐ Data files, or device/laptop have not been recovered ☐ Data at risk of further disclosure particularly through media or online

(ix) if the personal health information was adequately encrypted, anonymized or otherwise not easily accessible, and (c) any other factors that are reasonably relevant in the circumstances.			
Foreseeable harm from the breach (a) the sensitivity of the personal health information involved; (b) the probability that the personal health information could be used to cause significant harm to the individual, having regard for… (c) any other factors that are reasonably relevant in the circumstances.	☐ No foreseeable harm from the breach	Affected individuals: ☐ Loss of business or employment opportunities ☐ Hurt, embarrassment, damage to reputation or relationships ☐ Social/relational harm Public bodies and/or trustees: ☐ Loss of trust ☐ Loss of assets ☐ Loss of contracts or business ☐ Financial or legal exposure	☐ Security risk (ex. physical safety, unauthorized building access) ☐ Identify theft or fraud risk ☐ Hurt, embarrassment, damage to reputation may also be high risk depending on the circumstances ☐ Risk to public health or safety

January 2022