

ieMR Inappropriate Access – Severity and Actions Guide

The following criteria establishes the levels of severity and subsequent action following inappropriate access to ieMR by an employee.

Category Guide	Breach Severity	Action	CCC Recommendations
Blue	One or more instances of viewing patient with same surname when no direct relationship be established	Discuss with Line Manager to understand reason for access. <ul style="list-style-type: none"> If Line Manager substantiates access in accordance with role, no action to be taken, or If line manager doesn't substantiate access in accordance with role, access will be categorised into the below breach severity categories. 	If access is substantiated, then no reporting action is required.
Green	One instance of viewing self or immediate family with consent	An email is sent to the employee and an informal meeting with the Line Manager	<p>Level 2 (Section 40)</p> <ul style="list-style-type: none"> Repeated computer misuse (s 408E) that involves access only to the subject officer's own information / data or the information / data of immediately family (with consent), or unauthorised access by a subject officer to his / her own data after receiving a formal warning. IF there is any indication that the information gained has been used for any other purpose (i.e. family court matters, domestic violence, benefit or detriment to another) OR if an executive is involved THEN the matters become LEVEL 1 and dealt with accordingly. <p>Reporting Obligation</p> <p>The public official can commence dealing with these matters immediately and notify the CCC by way of a monthly schedule.</p>
Yellow	Multiple instances of viewing self-and/or immediate family with consent	Please Explain Letter issued to the employee and a formal meeting with Line Manager	
Orange	One instance of viewing of an ieMR record that is not connected with their official duties.	Please Explain Letter issued to the employee and a formal meeting with Line Manager	<p>Level 1 (Section 40)</p> <ul style="list-style-type: none"> Involves an offence of computer^[1] hacking and misuse under s408E of the Criminal Code where there has been an unauthorised disclosure; or systemic access to data held on a computer^[2] that would constitute a breach of that person's privacy (i.e. no consent) whether there has been a disclosure or not. <p>Reporting Obligation</p> <p>These matters are to be reported to the CCC without unreasonable delay. The public official may notify the CCC of the complaint by way of:</p> <ul style="list-style-type: none"> letter, email, or facsimile transmission <p>The public official must take no other action in relation to the complaint other than that which is required to:</p> <ol style="list-style-type: none"> maintain the integrity of any possible evidence, implement public interest discloser protection, or meet another statutory obligation under another act, including the referral of criminal conduct/allegations to the Queensland Police Service. <p>The public official may commence dealing with a matter notwithstanding its inclusion in this direction once 14 days has lapsed since the complaint was first provided to the CCC.</p>
Red	Multiple instances of viewing an ieMR record that is not connected with their official duties	Show Cause Letter issued to the employee	
Purple	Modified own ieMR medical record and/or other ieMR medical record that is not connected with their official duties	Show Cause Letter issued to the employee	

^[1] Computer – any device where data has been stored (a storage device); or any device that allows access to a storage device whether or not the storage device is held by the DCSYW i.e. 'cloud' storage, or access via a web portal to a database housed and / or maintained by another entity.

^[2] Ibid.