
Protecting Patients' Privacy

Joven Jeremius Q. Tanchuco, M.D.

The Implementing Rules and Regulations of Republic Act No. 10173, known as the "Data Privacy Act of 2012" was posted last August 25, 2016 which makes it official.^{1,2} Under the new law, doctors and other healthcare professionals fall under what is defined as a personal information controller or even a personal information processor. As doctors, we have long been aware of our moral duty to protect the most sensitive information pertaining to our patients. But with the law, breach of that obligation – unintentional though it may be – are now subject to penalties including hefty fines and even imprisonment, and sometimes even both.

Obtaining sensitive personal information from our patients is something we do every time we see patients. This is not only in relation to their illnesses, but other more personal details that may or may not impact our management of their diseases but have nonetheless come to our knowledge. Trust is a vital component of the patient-physician relationship. As our patients get more and more comfortable in this trusting relationship, they put their guards down. Oftentimes, they divulge details that we may not need or even ask for. Sometimes we may even get such information from people we have just met during a social gathering wanting to get some free medical advice. But because we now know about them, we now need to hold this information in strict confidence.

This may be more so when we need to deal with persons of prominence or position. Even such famous personalities get sick or would just need to consult with a physician regarding a matter which ails them. Political figures, celebrities, and other prominent individuals, including their loved ones and significant others do need to be taken care of as well. Sometimes, their illnesses or situations associated with their illnesses can impact their public image. At the least, their health – both physically and mentally – could be questioned. Supporters and fans may not like that their idols or even simple favorites are blemished with some imperfection even if it is not due to their wrongdoing. Particularly in a political and social landscape that is driven by personalities, leaders and other prominent figures who may no longer be perceived as strong or able to stay in their positions easily lose patronage. Thus, as we swear to Do No Harm to our patient when we treat them, we should also always aspire to do them no harm by not carelessly divulging any sensitive information that they have shared with us whether willingly or many times without even fully realizing it.

This need to protect a patient's most sensitive information, even if they are not celebrities or political figures, can sometimes run counter to the scientific undertaking that physicians need to also fully support as part of the learning environment. After all, it is only through the sustained conduct of such scientific endeavors do we hope to truly improve the lot of many of our patients in the future who are afflicted with disease. To be fair, the IRR does have certain provisions allowing for legitimate research to acknowledge that such activities should not be hampered, as long as proper safeguards and ethical considerations – including subject consent – are in place.

We would normally consider it sufficient precaution that as long as we have been able to eliminate the ability to link this potentially sensitive information to a particular individual, it is regarded as something which can be shared – a feature which many now apply the term "de-identify". In this regard, we should probably stop using the patient initials as part of case presentations or discussions even within the confines of an academic conference room. Coupled with the patient's sex and age data, and sometimes geographic location and occupation – items which can often be important in formulating diagnostic differentials – the patient initials make it easy enough if somebody were to really try, to actually trace who the actual person is. Those patient initials anyway, in my opinion, do not actually contribute to the scientific discussion which needs to take place.

The law as defined by the IRR also puts responsibility on anyone who may have become aware of such security breach to properly inform authorities or otherwise be subject to penalties as well. As we make our clinical rounds we see medical charts and other such patient records which can be easily seen or read by anyone. We should be more vigilant in reminding everyone, especially other members of the healthcare team that such should not be allowed to continue. Also, in many ways technology has helped a lot in our communication as well as information gathering and storage. However, with the law, we become obligated to protect that information. This covers sensitive personal information we have about our patients which we have in our cellphones, laptops, tablets, etc. If we lose these gadgets and have not taken security measures to prevent others from getting access to it, as personal information controllers we become liable.

A physician's obligation to protect a patient's privacy is upheld in the Hippocratic Oath – both the ancient as well as the modern versions. But with the Data Privacy Law of 2012, we can now be actually penalized for breach of this sacred trust. It is important we familiarize ourselves very well with the details of the IRR and identify the areas we may find relevant in our particular settings and practice. We should actively seek further guidance from the National Privacy Commission which has been tasked to provide education and even the technical standards to guide compliance with the law.

References

1. Republic of the Philippines. <http://www.gov.ph/2016/08/25/implementing-rules-and-regulations-of-republic-act-no-10173/>, 2016
2. Republic of the Philippines. <http://www.gov.ph/images/uploads/20160825-IRR-RA-10173-data-privacy.pdf>, 2016