



UNIVERSITY OF THE PHILIPPINES
Quezon City

OFFICE OF THE PRESIDENT

13 February 2019

MEMORANDUM NO. TJH 2019-07A

FOR: All Vice Presidents
Secretary of the University and of the Board of Regents

All Chancellors
UP PGH Director

SUBJECT: **Organizational and Technological Security Measures for Data Privacy Act Compliance (UPDATED)***

The University of the Philippines System Data Protection Officer during the OP Executive Committee Meeting on 14 January 2019 and the Presidential Advisory Committee Meeting on 17 January 2019 presented the highlights of privacy impact assessments she conducted and emphasized the need for the University to immediately implement the following organizational and technological security measures pursuant to the issuances of the National Privacy Commission - the body tasked to implement the Philippine Data Privacy Act (DPA):

**1. ESTABLISHMENT AND PHREB ACCREDITATION OF RESEARCH ETHICS COMMITTEES
OR BOARDS THROUGHOUT THE U.P. SYSTEM**

Constituent Universities (CU's) that still do not have Philippine Health Research Board (PHREB) accredited research ethics boards (REBs) or research ethics committees (RECs) are reminded to establish such bodies, provide the necessary support for the same and to have these bodies apply for Level 1 PHREB accreditation at the soonest possible time to enable researchers to process sensitive personal information (information relating to education, health, age/birth date, civil status, etc). pursuant to the opinion of the NPC that sensitive personal information is not covered by the exemptions listed under 4d of the Act.

Note the following provisions of the DPA:

Sec. 25 (b) The unauthorized processing of personal sensitive information shall be penalized by imprisonment ranging from three (3) years to six (6) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Four million pesos (Php4,000,000.00) shall be imposed on persons who process personal information without the consent of the data subject, or without being authorized under this Act or any existing law.

SEC. 34. *Extent of Liability.* – If the offender is a corporation, partnership or any juridical person, the penalty shall be imposed upon the responsible officers, as the case may be, who participated in, or by their gross negligence, allowed the

commission of the crime. If the offender is a juridical person, the court may suspend or revoke any of its rights under this Act. If the offender is an alien, he or she shall, in addition to the penalties herein prescribed, be deported without further proceedings after serving the penalties prescribed. If the offender is a public official or employee and he or she is found guilty of acts penalized under Sections 27 and 28 of this Act, he or she shall, in addition to the penalties prescribed herein, suffer perpetual or temporary absolute disqualification from office, as the case may be.

SEC. 36. *Offense Committed by Public Officer.* – When the offender or the person responsible for the offense is a public officer as defined in the Administrative Code of the Philippines in the exercise of his or her duties, an accessory penalty consisting in the disqualification to occupy public office for a term double the term of criminal penalty imposed shall be applied.

The Philippine National Health Research System (PNHRS) Act and National Ethical Guidelines on Health and Health Related Research 2017 (NEGHR) define health broadly such that social research and other research will fall under the definition of “health research” and “health related research” under the PNHRS law

<https://www.officialgazette.gov.ph/2013/05/07/republic-act-no-10532/>, its IRR

<http://www.ethics.healthresearch.ph/index.php/component/content/article/2-uncategorised/214-implementing-rules-of-pnhrs> and the NEGHR

<http://www.ethics.healthresearch.ph/index.php/phoca-downloads/category/4-neg>.

Further note that CHED Memorandum Order No. 52 Series of 2016 (p. 20) requires HEIs to adhere to the NEGHR.

UP as the National University must provide conditions, including effective and efficient ethics review processes needed by our researchers in order to be able to obtain funding for research and development, to present research findings in conferences and other similar public fora and through publications so as to be able to comply with the requirements for tenure and promotions for University personnel and academic requirements for our student researchers. CUs are encouraged therefore to establish several RECs or REBs that will review various kinds of research and to have the same PHREB accredited, as UP offices and other funding agencies, organizers of public fora, editorial boards of journals and the like require ethics clearance. (See Appendix E PHREB policies and Requirements for the Accreditation of Research Ethics Committees, Coverage No. 1 Academic Institution based RECS, p. 190).

Please refer to the NEGHR 2017 <http://www.ethics.healthresearch.ph/index.php/phoca-downloads/category/4-neg> for more information and/or visit the PHREB site <http://www.ethics.healthresearch.ph/index.php/registration-and-accreditation>.

2. COMPULSORY USE OF U.P. MAIL IN ORDER TO ACCESS UNIVERSITY DATA PROCESSING SYSTEMS ONLINE

The entire UP community (students, alumni, University personnel and officials) must use UP mail in order to transmit email to UP offices and access UP data processing systems such as the University Information Systems, Computerized Registration Systems of CUs and the like and activate two step verification at the soonest time possible. For information about how

to apply for UP mail please see <https://itdc.up.edu.ph/uis/faqs>. Aside from DPA compliance, we encourage currently enrolled students and currently employed faculty and staff to use UP mail and avail of Microsoft Office 365 through their UP mail accounts. Refer to <https://itdc.up.edu.ph/uis/microsoft-office-365-for-up> for more information.

The UP System Office of Alumni Relations and Chancellors are requested to remind the proper CU offices to require alumni to apply for a UP alumni account by filling up the alumni update form at <https://alum.up.edu.ph/database/>.

For information regarding two step verification kindly refer to <https://www.google.com/landing/2step/index.html#tab=how-it-protects>. The UP community will have a grace period of thirty (30) calendar days to apply for UP mail (if they do not have an existing account) and activate 2 step verification counted from the date of the official release of this memo. We request the Chancellors to please see to it that the proper offices send a copy of this memo via email to the persons concerned and to post this memo in the appropriate sites of the CU such as the home site of the CU, site of the University Registrar, HRDO and such other sites that members of the UP community are likely to access so that they will be able to read and comply with this memo. The administrators of relevant U.P. System sites are likewise enjoined to post this memo.

The Chancellors are requested to remind relevant offices such as the University Registrar, HRDO and their respective IT offices to see to it that those who have registered email addresses other than UP mail be immediately notified that they will no longer be allowed access to UP data processing systems except through the UP mail accounts after the thirty (30) calendar days grace period mentioned below.

After the thirty (30) calendar days grace period, UP ITDC as the UP-mail administrator will set two step verification by default such that users will have no choice except to use such method in order to access their accounts. The proper System Offices and Chancellors are requested to issue the proper memo, email and/or sms notices so that the community may be immediately apprised of such requirement.

3. REMINDER TO AVOID SENDING SENSITIVE PERSONAL INFORMATION VIA EMAIL

All UP mail users are reminded to avoid sending as far as practicable sensitive personal information such as confidential educational records, information related to health as well as disciplinary cases. In the event such cannot be avoided users must ensure that the email and files transmitted are encrypted at rest and during transmission. Note that UP mail does not meet this standard and therefore additional encryption tools must be used. Please refer to <https://chrome.google.com/webstore/search/encryption%20for%20gmail> for examples of tools that can be used to encrypt UP mail and email attachments. UP ITDC as well as other email administrators throughout the System should take such reasonable steps given their resource and other constraints to enable the UP community to comply with this recommendation and the mandatory NPC requirement re encryption at rest and during transmission. NPC recommends the use of AES 256.

4. REMINDER THAT PASSWORDS SHOULD NEVER BE SHARED, SHOULD BE CHANGED PERIODICALLY AND THAT STRONG PASSWORDS BE USED

Users should be reminded that they should never share their passwords. It is also good practice to change passwords periodically and to follow the IT Office advisories regarding how to make strong passwords. System and CU offices must develop mechanisms in order to ensure that personnel who are unable to input data using their own passwords do not share their password to others and instead request the proper heads of unit in writing for administrative staff to input such data using the administrative staff's own account. Such letter must clearly state that the requesting party assumes liability for any error in the entry of data such that in the case of change of grades for example it is the faculty or lecturer requesting administrative staff to input grades who still assumes accountability for the error. The System Offices and Chancellors are enjoined to remind units to request separate administrator accounts if various officials and/or personnel need to use administrator accounts so as to further ensure accountability.

The relevant CU offices that do not use SAIS at present must coordinate with the proper IT offices to ensure for instance that faculty who are graduate students are not able to use their accounts as faculty in order for example to view grades, enlist or delete the enrollment of students in graduate courses etc.

5. MANDATORY USE OF TWO STEP VERIFICATION OR MULTIFACTOR AUTHENTICATION IN ORDER TO ACCESS UNIVERSITY DATA PROCESSING SYSTEMS ONLINE

UP ITDC as well as CU IT offices are again reminded to act with all due and deliberate speed in ensuring that the University will be able to comply at the soonest time possible with the requirement that all who access personal data online must do so through a secure encrypted link and use multi factor authentication. Such IT offices were apprised of such requirement by the UPS DPO during the UP IT Summit held in January 2018.

6. HRDO DUTY TO INFORM I.T. OFFICES ONCE PERSONNEL CEASE TO BE CONNECTED WITH THE UNIVERSITY AT THE SOONEST POSSIBLE TIME SO THAT ONLINE ACCESS AS WELL AS SECURITY CLEARANCES FOR DATA CENTERS CAN BE IMMEDIATELY REVOKED

HRDOs throughout the entire System must furnish the proper IT offices as well as data centers e.g. offices that have custody of student and personnel records for example, the name(s) of University personnel who cease to be connected with UP in order to enable the latter to immediately revoke the credentials or security clearances used to access UP data processing systems and data centers.

7. REVISIONS TO REGISTRATION SYSTEMS IN ORDER TO PREVENT STUDENTS FROM DISCLOSING SPECIFIC HEALTH INFORMATION WHEN DROPPING OR APPLYING FOR A LEAVE OF ABSENCE, ETC.

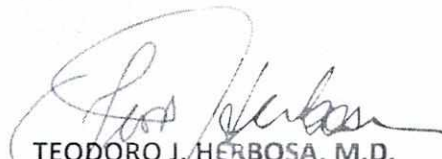
The Chancellors are requested to remind IT Offices to revise registration systems such that drop-down boxes stating the reason for dropping, applying for LOA and the like will use the broad term health reason in order to prevent students from disclosing specific health information in such registration systems. The relevant site should instead require students to submit the proper letter and medical certificate to the proper University offices that must put in place physical, organizational and technological measures to safeguard the right to privacy of students.

8. CONSTITUENT UNIVERSITY DATA PROTECTION OFFICERS MUST CONTINUE TO PROVIDE THE NECESSARY DPA TRAINING, CONDUCT PRIVACY IMPACT ASSESSMENTS AT THEIR OWN LEVEL AND SUBMIT REPORTS TO THE UP PRESIDENT AND UP SYSTEM DATA PROTECTION OFFICER AND THROUGH THE OFFICE OF THE SECRETARY OF THE UNIVERSITY

Finally, CU DPOs are also reminded to continue to provide relevant and up to date DPA training and conduct their own privacy impact assessments especially for systems which process sensitive personal information that are under their respective jurisdictions and to submit such reports as well as security incident or data breach reports to their Chancellor and to furnish a copy of such reports to the Office of the UP President and the UP System Data Protection Officer through the Office of the Secretary of the University in order among others to enable the crafting of Systemwide policies and procedures that take into account the conditions and experiences of the CUs and other relevant factors.

Kindly await the issuance of subsequent memoranda regarding the holding of joint DPO and IT office meetings and workshops to update the existing common training modules to be used by all DPOs and for the discussion of among others the latest version of the Draft UP System Data Privacy Policy, Proposed Revisions to the Acceptable Use Policy, Draft I.T. Security Policy and PIA forms and notices for CCTV operation throughout the UP System as well as the Non-Disclosure Undertakings to be signed by all University personnel as well as those engaged by UP through a contract of service.

For your immediate compliance.


TEODORO J. HERBOSA, M.D.
Executive Vice President
By authority of the UP President

**Italicized and underlined texts were added.*