University Hospital is fully committed to protecting the privacy and security of our patients' information. This notice is regarding a cyber incident we identified involving some patient information.

On September 14, 2020, as part of our ongoing cyber monitoring program, we became aware that an unauthorized individual may have gained access to the Hospital's computer systems containing patient information on September 10, 2020. We took immediate, aggressive steps to contain the incident and investigate the cause and extent of the event with assistance of leading privacy experts and law enforcement. Following a comprehensive review of all impacted computer files, we determined that some patient information may have been contained in the files, including patients' names, patient demographic information, health insurance information, and/or clinical information. Additionally, for a limited number of patients, social security numbers, driver's license or state identification card numbers, passport numbers, and/or financial account information was also included. University Hospital has no reason to believe any of the information has been further used.

We have no reason to believe any patient information has been further used. However, we began mailing letters to patients whose information was contained in the impacted computer files on November 12th, 2020 and are offering free credit monitoring to individuals who have a social security number, state identification number or passport number included in their account. Additionally, we have also established a dedicated call center to answer any questions about this incident, which may be contacted at 833-971-3219, 9am to 6pm, Monday through Friday, Eastern Time.

We want to assure you that we take this matter very seriously. We deeply regret that this incident has occurred and greatly value the trust you have placed in University Hospital. We recommend patients review the statements they receive from their health care providers. If patients see charges for services they did not receive, please contact the provider immediately. Please be reassured knowing that we have further enhanced our security protocols in response to this event, in order to reduce the likelihood of a similar event from occurring in the future.