LIONS GATE HOSPITAL FOUNDATION

For Immediate Release **August 4, 2020**

IMPORTANT NOTICE TO DONORS: Blackbaud Data Breach

Lions Gate Hospital Foundation wishes to inform its valued supporters about a recent incident that affected some of the personal information that has been entrusted to us.

On July 16, 2020, we were notified by one of our service providers, Blackbaud that it had recently fallen victim to an attack on its computer network that impacted many of its clients worldwide, including the Foundation. Fortunately, this backup file did not contain any credit card or any personal financial information, which we encrypt (make unreadable) and store separately. It did, however, contain some other personal information, as explained below.

We are committed to protecting the personal information entrusted to us, which means that when an incident like this happens that may put donor information at risk, we tell you about it. We also want to explain what we are doing to respond to the incident and protect you, what the nature of the risk to you might be, and what you can do to protect yourself.

What Happened?

Blackbaud is one of the world's largest providers of fundraising and financial management software to non-profit organizations. On July 16, 2020, Blackbaud notified us that it had discovered the attack in May 2020. The particular type of attack against Blackbaud is known as a "ransomware attack" because the criminal accesses the victim's computer network and either encrypts or steals a copy of databases or files and then demands a ransom payment in order to de-encrypt or return them. Blackbaud informed us in the same notification that working together with cybersecurity expert advisors and law enforcement, it had (1) prevented the criminal from accessing most of its computer network and shut down the criminal's access to its computer network, (2) paid the criminal's ransom demand in return for a promise from the criminal that they would destroy the copies of the stolen databases and files and not sell or use them for any purpose. Based on advice from its cybersecurity

expert advisors and law enforcement, Blackbaud is satisfied that the criminal will keep their promise.

The Foundation was not consulted about any of Blackbaud's decisions about how to handle the incident. We were simply told about the attack and what decisions and actions Blackbaud made and took in response. We also don't share Blackbaud's confidence that criminals keep their promises.

What Personal Information was taken?

The Foundation applies very strong security measures, such as encryption, to protect sensitive financial information. We can confirm that donor financial information was not stolen or accessed by the criminal. Unfortunately, the criminal was able to steal a copy of a backup file that contained the following elements of personal information (if you provided any of these to us): name, address, phone number, email address, marital status and date of birth, as well as donation history, attendance at our events and communication preferences.

We do not know whether the criminal has actually looked at any of the information contained in the stolen file; we only know that the file itself was stolen.

Please be assured that the Foundation's donor data is completely separate from Vancouver Coastal Health's patient database. Patient information was in no way compromised as a result of this incident.

What is being done to protect your Personal Information?

Blackbaud paid the ransom demand to try to ensure that the stolen information is destroyed and is not sold or otherwise further misused. Blackbaud has also hired a third party team of experts to monitor the Internet for any evidence that the stolen information is being offered for sale. For our part, since we were notified of the incident, we have engaged our own privacy and cybersecurity experts to advise us on how to best protect you and comply with our obligations under British Columbia's *Personal Information Protection Act*. One further step we are taking, in addition to this notice, is to notify the Office of the Information and Privacy Commissioner for British Columbia ("OIPC") about this incident.

What can you do to protect yourself?

Please be cautious in responding to any communication you receive, whether a letter, phone call or email, that asks you to provide your financial information, account access information or other sensitive information, until you can confirm that the communication is legitimate. In particular, if you receive an email from us, or from any organization or individual that you weren't expecting, do not open any attachments or click on any links until you have verified the sender's identity. You can do this in an email by hovering your cursor over the sender's name so that you can see the sender's full email address. All staff email addresses have the following structure: Firstname.Lastname@vch.ca. Our official Foundation email address is info@lghfoundation.com. Any email that says it is from us where the sender email address does not have this structure or does not come from the official Foundation address is not legitimate. Do not open any attachments or click on any links and delete the email.

Who can you contact for further information?

We sincerely apologize for the fact that this incident occurred and that it has impacted you in any way. If you have questions or concerns that have not been answered in this notification, please do not hesitate to contact the Foundation at 604.984.5785 or by email, info@lghfoundation.com.