

## **AB0602 Writing Pre-test**

### **Instructions**

This pre-course writing test is to be completed by **12 noon, 11 January 2020** (Monday). Submit your script via the *Assignments* folder in your AB0602 Seminar Group Site.

Before uploading your script, make sure that you:

- State your name and Seminar Group number at the top of your script
- Save it as a Word document, using this filename format: **Pretest\_SemGrp\_Name** (e.g., *Pretest\_Sem03\_AlexGoh.docx*)

Your submission must be your original work. The Turnitin tool in NTULearn will identify drafts with a high degree of similarity to other works.

***Note: If you should change Seminar Groups, please resubmit your script and inform the tutor of your new group***

## **Thomas Bingley Medical Group: Data leak crisis**

### **Background**

Thomas Bingley Medical Group (TBMG) is a leading integrated private healthcare provider in the Asia-Pacific region, operating medical facilities in 10 cities across five countries and territories including Singapore, Beijing, Hong Kong and Kuala Lumpur. It is the only private medical provider in Singapore to own and operate a fully integrated healthcare organisation comprising hospitals, a network of family medical and dental clinics, Traditional Chinese Medicine clinics, and a consumer healthcare division.

Founded in 1971 with just one clinic in central Singapore, TBMG has grown over the years to serve over 2 million patients today and more than 5,800 corporate clients each year. Today, TBMG has a staff strength of 2,000, including 290 physicians.

From primary care at its network of Thomas Bingley Medical Clinics to specialist and tertiary care at Thomas Bingley Hospital, the Group prides itself on offering a seamless continuum of care to all its patients. In addition, over the last 10 years, the Group has built a reputation for attracting and treating high net worth (HNW) patients from neighbouring countries, the “cream” of the medical tourism market that Singapore has aggressively tapped into as a lucrative market.

TBMG states that its mission is to “Enhance health and well-being by providing the best total healthcare” while its vision is to be their patients’ “Trusted partner for health”. The Group’s core values include:

- Compassion – Putting patients and their well-being at the centre of all the group does, treating all with respect, compassion and dignity
- Commitment – Upholding patients’ trust by maintaining the highest professional integrity and standards
- Excellence – Continually seeking advancement and innovation to achieve better healthcare
- Team-based care – Dedicating and combining skills, knowledge and experience across the Group for patients’ benefit
- Value – Seeking always to create and deliver value for patients

### **Senior Management Team**

Three years ago, Dr Julian Wong Meng Teck was appointed Group CEO and Executive Chairman of TBMG. A highly reputed cardiologist and one of the top surgeons in his field worldwide, Dr Wong is known to be a conservative surgeon with a meticulous and cautious personality.

Dr Wong’s management team comprises:

- Dr Ang Seng Poh, Chief Operations Officer
- Ms June Koh Yi Ting, Chief Financial Officer/Company Secretary
- Ms Marilyn Teo Su Lin, Director, Commercial Affairs
- Mr Phua Kah Leong, Chief Information Officer

### **The Situation**

It was only 9am on Monday, 4 November, and the Group’s Director for Commercial Affairs, Marilyn Teo, was already in her office looking through the weekend’s media clips and social media report sent through by their monitoring agency. As the most senior executive responsible for TBMG’s reputation and external engagement, Marilyn was always conscious

of the need to keep an eye out for incidents and events that could impact the Group and the healthcare sector.

The fact was the sector had been taking a beating in recent years. In particular, three major incidents tainted the industry:

1. In July 2018, Singapore suffered its largest data breach ever in the healthcare industry, when the personal information of 1.5 million SingHealth patients was leaked. Embarrassingly for SingHealth and the whole industry, patients affected included the Prime Minister and several cabinet ministers.
2. Barely 6 months later, in January 2019, the Ministry of Health (MOH) announced that confidential information belonging to over 14,000 people diagnosed with HIV had been stolen and leaked online.
3. Then, in March 2019, 808,201 blood donors in Singapore had their personal details exposed. These donors had their NRIC (personal identity card issued to all Singaporeans) number, gender, number of blood donations, dates of the last three blood donations, and in some cases, blood type, height and weight, leaked online for 2 months until a cyber-security expert found the loophole and informed the authorities.

Just as Marilyn was reflecting on how TBMG had managed not to be embroiled in crisis or negative publicity so far, her office phone rang. She could tell from the caller ID that it was Wendy Lim, Personal Assistant to the Group CEO and Executive Chairman.

Wendy informed her that Dr Wong was calling for an urgent senior management meeting in half an hour. What could be so pressing, Marilyn wondered as she quickly glanced through her media clips and social media report again to make sure she had not missed anything.

Marilyn walked into the boardroom five minutes early but could see that the other three members of the senior management team were already seated. Just as Marilyn started greeting everyone, Dr Wong strode in purposefully.

Dr Wong: Everyone, please get seated quickly. We have something very urgent and crucial to discuss. Kah Leong, can you start?

Kah Leong: Eh, yes. Thank you, CEO. Eh, I'm afraid I have some bad news...

Dr Wong: For goodness' sake, get on with it!

Kah Leong: Yes, yes, alright. Eh, we had a bit of a problem over at IT. We discovered a data breach over this past weekend...

Dr Ang: Oh my goodness. What kind of breach?

Kah Leong: Well, to put it simply, someone hacked into our IT system and took patient info...

June: What exactly did they take?

Kah Leong: We are still trying to confirm this but it doesn't look good so far. We think the hacker or hackers managed to get personal data including names, identity card and passport numbers, addresses, contact details and other personal info such as date of birth, as well as medical data like diagnosis and treatment history.

Marilyn: Meaning to say... this is worse than the SingHealth leak because that only involved personal data, not medical.

Kah Leong nodded solemnly.

Marilyn: But exactly how many of our patients are affected? Surely not all 2 million across the region?

Kah Leong: No, no, just 10,000 patients.

June: That's not too bad, right?

Marilyn: True, the number doesn't appear huge but a breach is still a breach.

Dr Wong: I'm sorry to tell you all that the picture is far bleaker than that. What Kah Leong hasn't said yet is that the culprit was very selective with which 10,000 patients to target.

Kah Leong: Yes, CEO is right. He or she appears to have downloaded the info of our top 10,000 paying patients. In other words, the ones who had the most expensive treatments or procedures, or those who required the attention and use of the most expensive specialists, equipment or facilities.

Dr Ang: Exactly how is this sort of info reflected in their records?

June: I can answer that. As you all know, many of our top-paying patients are non-Singaporeans. So with this group, aside from payment card numbers and expiration dates, we would typically ask for additional financial records or proof of ability to settle their bills, such as bank statements. You must remember that such bills can often go into seven figures.

So, are we saying such sensitive financial records were stolen?

Dr Wong: Yes, exactly that! If the financial records of these patients get leaked publicly as a direct result of this breach, TBMG would be in big trouble. And that's a huge understatement.

Marilyn: We could get sued. By some of the richest people in Asia, at that!

Dr Ang: Do we even know how this breach happened?

Kah Leong: We still don't know. The fact is we have invested in the best IT security systems available in the market. In fact, I swear on my life that we actually pump in way more money into our systems than even the public medical groups like SingHealth or MOH, for that matter.

My department is also the largest team of IT experts ever assembled in this region to support a private healthcare organisation. Aside from the actual systems hardware and solutions, we have very robust maintenance and prevention procedures in place.

In fact, it was our advanced monitoring system running its fortnightly check last night that discovered the breach and sounded the alarm. It detected anomalies indicating that confidential patient info had been downloaded.

- Dr Wong: Needless to say, Kah Leong, you need to do an immediate review of our systems and procedures to understand how this breach happened and what we can do to prevent this from happening again.
- Kah Leong: Understood. I've already got my team leaders urgently working on a comprehensive review.
- June: Back to the main problem. How exactly are we going to explain what happened publicly, especially to the affected patients?
- Marilyn: Yes, according to Ministry of Health guidelines, when such a large number of patients are involved, we must issue a press statement to inform the public via mainstream media.
- June: Does that mean the affected patients will find out that their personal and medical records have been stolen only when they flip through their newspapers over breakfast? Surely, we need to give them some kind of heads-up?
- Marilyn: It doesn't have to be that way. In cases like this, the organisation involved can choose to send an email to the affected patients before they inform the general public through the media. We should plan on doing exactly this, with your agreement, CEO?
- Dr Wong: I definitely agree. We at least owe it to our patients to let them know first.
- Marilyn: Oh my goodness...
- June: What's wrong, Marilyn?
- Marilyn: It's just that... I got an email from the Customer Service Team Manager over the weekend. He reported that two former patients received phone calls just yesterday supposedly from our call centre asking for personal info. The manager claims that none of his team members was tasked to make such requests. Could this be somehow connected to the hacking?
- June: All the more we need to send that email out ASAP.
- Dr Ang: We need to be really careful how we craft this email. How will we tell the patients such bad news without upsetting them or worse, getting sued by them?
- Dr Wong: I'm sure Marilyn and her team can get it done. What else do we need to do? How about reporting the incident to the police?
- Kah Leong: Seng Poh and I will be making the police report after this meeting. CEO, in cases like this, it is prudent to hire an external digital forensics and security firm to assist us with the internal investigation. Can I have your OK to do this?
- Dr Wong: Yes, go ahead.
- Dr Ang: Just thinking aloud – is there any way we can soften the blow?
- Kah Leong: Maybe we can offer the patients a 10 percent discount off any future consultations or treatment? As a goodwill gesture?

June: Are you really sure that's appropriate, Kah Leong?

Dr Wong: Right Marilyn, we need to see a draft. When can it be ready?

Marilyn: I will drop everything and get it to you after lunch.

Dr Wong: All right then. We will reconvene later today to go through Marilyn's draft.

**Task**

You are an Executive at TBMG reporting to Marilyn. She has tasked you to draft the email to affected patients. She needs to see it in 2 hours' time so that she can review it before the follow-up senior management meeting.