Appointment & Scheduling Management Information System

Overview

Queens Medical Center currently uses telephone-based office assistance for scheduling appointments, resulting in numerous delays providing patients access to the clinic's medical specialists. Office assisted scheduling presents difficulties for prospective patients with limited telephone access during clinic hours, constrains simultaneous appointment scheduling and is an inefficient utilization of medical office staff (Zhao, et al., 2017). Delays to medical specialist access will continue to degrade as Queens' catchment area community populations increase. Therefore, an internet-based, patient self-scheduling application has been recommended.

Patient experience, wait times and clinic operations can all be improved with online self-scheduling systems (Relatient, n.d.). Studies have also shown shorter wait times and self-scheduling reduce no-show rates, (patients missing appointments without notice) (Marhefka, 2020; Zhao et al., 2017). Scheduling system improvements optimize medical specialists' clinic hours availability and spread fixed costs (Froehle & Magazine, 2013).

Reducing patient wait times and improving clinic efficiencies are Appointment Scheduling Management Information System (ASMIS) implementation positives. The proposed system's internet exposure and personal health information breach consequences (Georgiou & Lambrinoudakis, 2021) raise risk concerns. Consequently, Queens management have requested a cyber threats and mitigation option assessment (University of Essex, 2021).

ASMIS Benefit Analysis

Queens Medical Centre requires more patient-centric appointment scheduling, proposed use cases are illustrated below. Although ASMIS will change Queens operational activities, benefits analysis is focused on patient experience and clinic operations (Fix, et al., 2018).

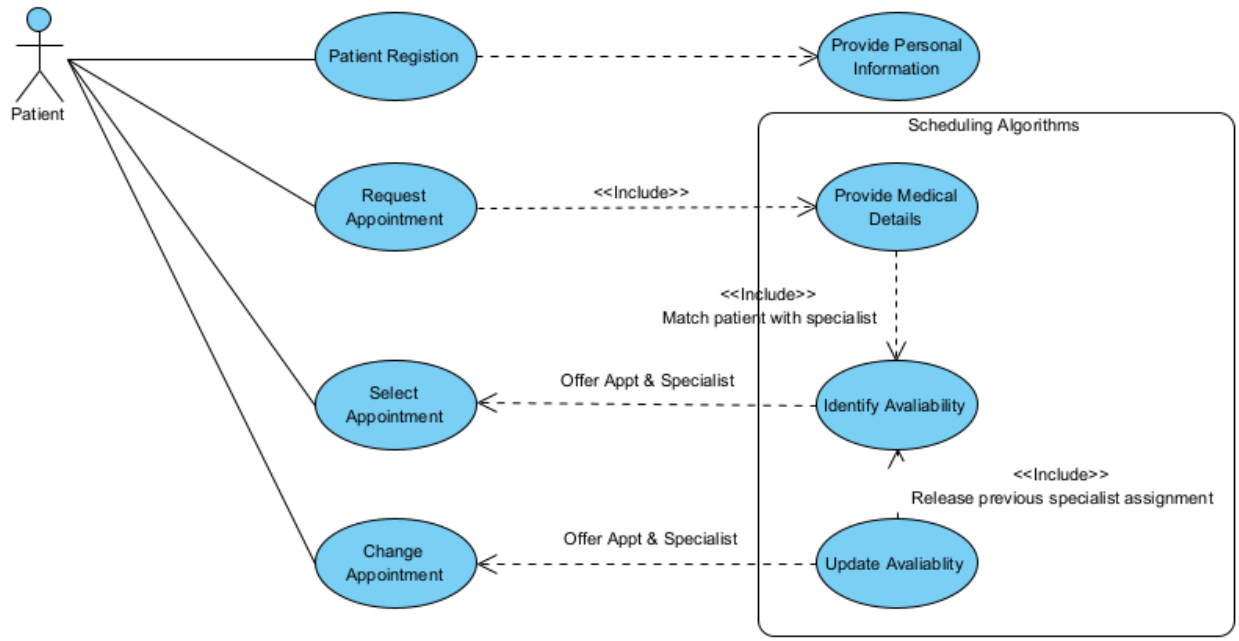

Figure 1 Patient-centric ASMIS Interactions

Patient Registration:

- Self-registration via internet application removes clinic hours constraints.
- Beyond patient convenience, self-registration enables medical office staff reallocation to higher value clinic work (Relatient, n.d.).

Provide Personal Information:

- Electronic form-based collection increases data quality by removing transcription errors occurring during patient communication with medical office staff simultaneously performing data entry (Lane, et al., 2006).
- Data input by the patient also reduces casual exposure to confidential information such as overheard medical office staff conversations.

Request Appointment:

- Appointment requests trigger medical information collection and consultation appointment scheduling. Patient interaction with ASMIS will resembles other online services, insulating the patient from clinic logistics.
- Patient-centric medicine expectations dictate arranging a medical appointment should be similar to purchasing movie tickets (IBM, 2019); expedient and self-directed.

Provide Medical Details:

- Studies of patient self-scheduling software have identified patients disclose sensitive medical matters more accurately through online portals than medical office staff conversations (Zhao, et al., 2017).
- Data quality and accuracy improvements assist consulting specialists' preliminary assessments and can aid scheduling algorithms.

Select Appointment, Change Appointment:

- Patients using ASMIS for appointment selection and changes frees medical office staff for higher value clinic work.
- Self-scheduling studies indicate a reduction in no-show rates, lowering the overall cost of care (Marhefka, 2020).

Both academic (Froehle & Magazine, 2013) and commercial (Relatient, n.d.) entities identify schedule optimization as a means of improving clinic efficiency and reducing operating costs. Therefore, use cases that balance clinic specialist workload (University of Essex, 2021) have been prioritized.

Identify Availability:

- Computerized scheduling can identify appointment options based on search criteria.
- Key words derived from the patient's request or symptom description allow viable specialist selection.
- Patient preferences like specialist gender or language can be combined to provide appointment times and specialist choices without additional workload for medical office staff.

Update Availability:

- Medical specialist availability changes due to cancellation or rescheduling can be immediately cascaded.
- Short notice cancellation losses may now be recoverable through patients amenable to moving appointment times (Relatient, n.d.).

ASMIS Cyber Security Threat Modeling

Mitigating all foreseeable risk is not feasible, consequently threat modeling methodology guidance developed by Microsoft (Howard & LeBlanc, 2002) will be used to identify, prioritize, and analyze potential risk mitigations. Queens Medical Centre management have specific concerns regarding patient data protection from cybercriminals (University of Essex, 2021). The likelihood of attack, combined with regulatory and reputation impacts, justify this risk prioritization.

A 2018 global security report showed health care records garnered the highest black-market prices (Trustwave, 2018) making internet facing medical systems lucrative targets. The Information Commissioner's Office has indicated the Data Protection Act 2018 remains in force post Brexit and most GDPR principles (Information Commisioner's Office, 2020) will apply. Therefore, as a data controller and processor Queens could expect fines of several million Euros (GDPR.EU, 2021) with an ASMIS data breach.

Since the ASMIS application is early in development, initial threat modeling will incorporate abuse cases. Abuse cases extend the use case approach, considering how adversaries might compromise a system (McDerrmott & Fox, 1999). Like use cases, abuse cases are suitable for discussions with Queens management or technology teams and easily revised when new requirements are identified or change (Tarandach & Coles, 2020). Figure two illustrates three attack categories initiated by cybercriminals attempting to compromise the ASMIS application.

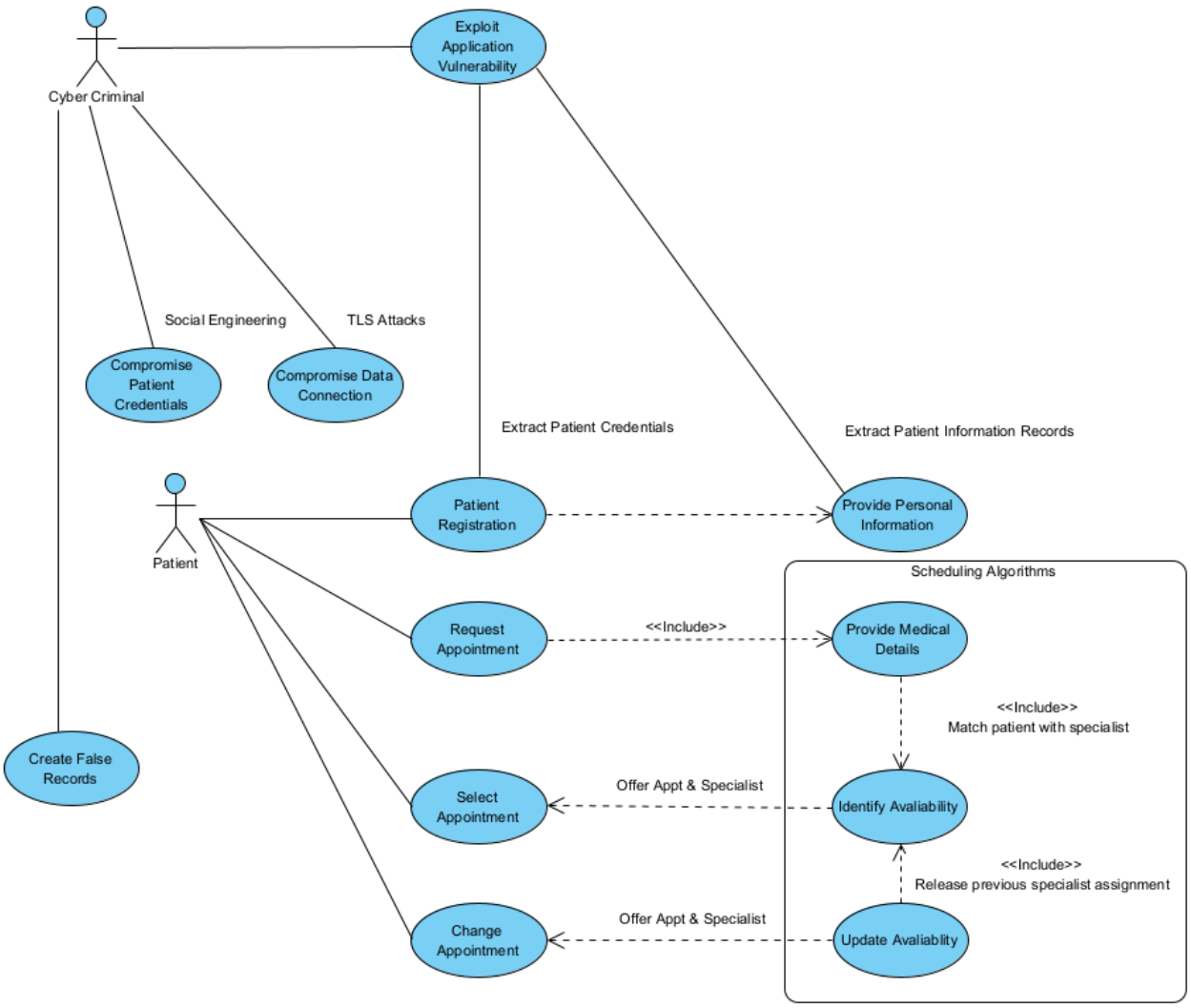

Figure 2 External Attacker Abuse Cases

Exploit Application Vulnerability:

The abuse case context is a vulnerability within the ASMIS application enables an adversary to extract multiple patient records or credentials. The 2021 Verizon Data Breach Report (VDBR) states web application attacks continue to be prevalent and financially motived (Verizon, 2021), therefore ASMIS application must be secured against high likelihood and high impact web application attacks. Additional threat modeling using an enhanced STRIDE methodology (Shostack, 2014), detailed in the next report section, will be used to provide this assurance.

Create False Records:

An attacker creates multiple fake profiles then uses online appointment booking to deny legitimate patients access to care. This scenario is somewhat unique to ASMIS, a variant of second order of denial-of-service attacks (Oswaldo, et al., 2015) enabled by web application business logic vulnerabilities (OWASP Foundation, n.d.).

Compromise Patient Credentials:

Although credential loss through social engineering is more common than web application exploitation (Verizon, 2021), impact is typically lower than bulk data loss. Individual account compromises must still be mitigated though, they reflect negatively on Queens Medical Centre and an administrative account compromise would be extremely detrimental.

Compromise Data Connection:

Patient communication with the ASMIS application is internet-based and must be encrypted to prevent network sniffing attacks. Transport Layer Security (TLS) is the common remedy but not impervious to attack (VENAFI, n.d.), although such attacks are difficult to perform against multiple victims.

Detecting attacks from trusted insiders is difficult, electronic systems record access events not intent. Information protection measures for patient data must include administrative controls such as audit review (Canadian Centre for Cyber Security, 2020). Figure three illustrates attacks that could be initiated by information technology (IT) administrators or medical office staff (MOS) using their ASMIS access to target patient data.

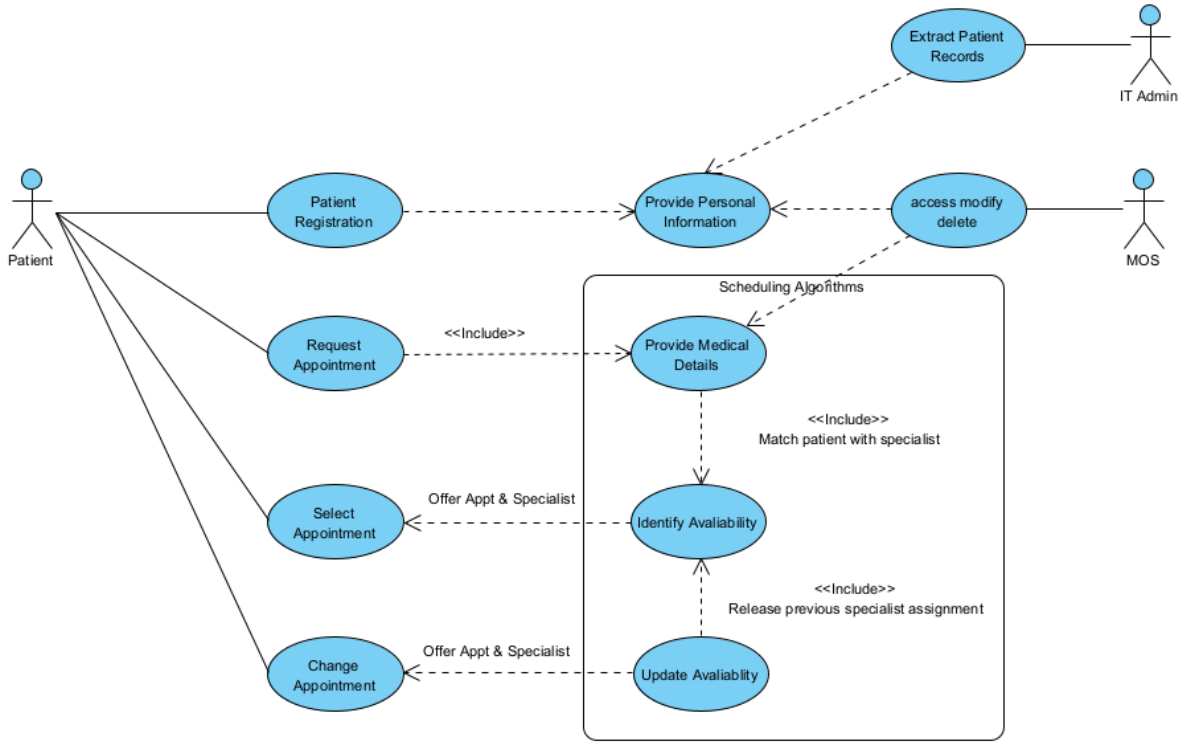

Figure 3 Trusted Insider Abuse Cases

Extract Patient Records:

- A database administrator or server administrator copies all patient records in a database then leaks the data.

Access Modify Delete:

- A medical office staff member looks up contact information or recent health history for personal or financial reasons.
- A medical office staff member changes information or deletes records altogether for personal or financial reasons.

STRIDE Analysis

Application exploitation was identified during abuse case analysis as the primary risk to be mitigated. Therefore, STRIDE, Microsoft's application-centric threat modeling approach (Howard & LeBlanc, 2002), will be foundational to determining effective cyber security technology controls. Microsoft's Adam Shostack later utilized trust boundaries to define threat modeling scope, asesseing security controls where different privilege level entities interact or exchange data (Shostack, 2014). The ASMIS trust boundaries illustrated below have been assessed using the STRIDE methodology.

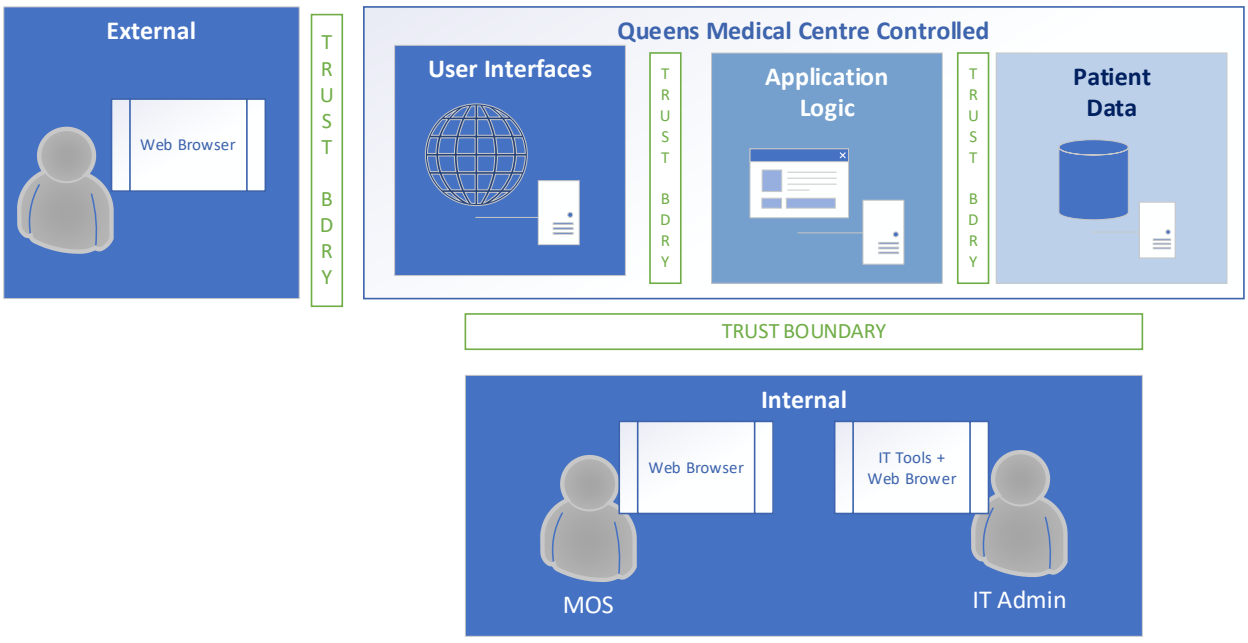

Figure 4 ASMIS Trust Boundary Model

The trust boundary between internet sources and ASMIS user interfaces is the initial point of an attack for any external cybercriminal. The recommended first layer of protection is an HTTP security application gateway such as the Amazon Web Services web application firewall (WAF) (Amazon Web Services, 2021). WAF technology blocks website attacks such as cross site scripting, code injection and all traffic from known malicious sources. WAF limitations are suspicious patterns identification within HTTP requests and can be bypassed by a motivated attacker but still provide effective preliminary defence against STRIDE threat categories Tampering and Denial of Service.

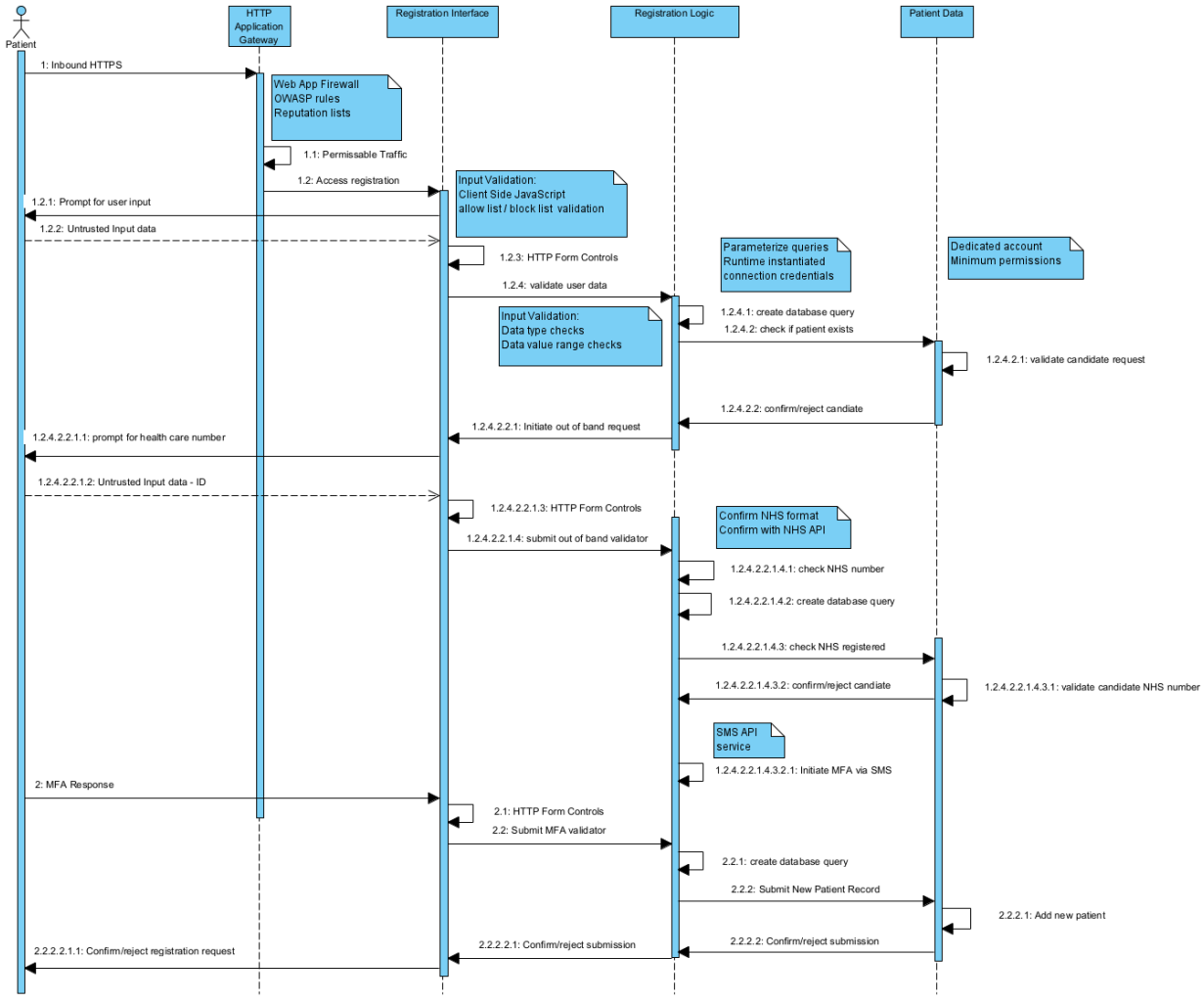

Figure 5 ASMIS New Patient Registration (negative responses omitted)

A WAF can test all HTTP requests before allowing connection to ASMIS webservers but dropping known malicious traffic at ingress is only a preliminary filter, it does not remove the need for additional layers of input validation. All input fields on ASMIS user interface pages will use JavaScript validation to provide a second defense layer (OWASP Foundation, 2018). Unfortunately, motivated attackers can bypass JavaScript controls (Offutt, et al., 2004), necessitating a third defence level of input validation performed by ASMIS application servers (OWASP Foundation, 2018). Application server programs must validate data types and value ranges then generate parameterized queries for input into patient database tables. Parameterized queries are considered the most reliable prevention measure for SQL injection attacks (OWASP Foundation, 2020). The three layers of input validation are designed to prevent tampering threats associated with the code injection attack class (Zhong & Rezos, n.d.) which left unchecked can manifest as STRIDE threat categories Information Disclosure and Elevation of Privilege.

ASMIS self-service registration is the most challenging to secure because it must accept input without first positively authenticating the source. This requirement opens spoofing attack possibilities, due to a lack of repudiation, resulting in a business-based denial of service condition. This attack vector must be managed through application business logic and restricting which entities can access the patient database.

Three separate checks are recommended prior to allowing new patient registration. First confirm patient name and contact information is not previously registered. Second, each new user registration must be associated with only one National Health Services (NHS) number for a non-deceased person not already assigned to another Queens' patient record. Validation can take place near real time via NHS application programming interface (API) requests (NHS Digitial, n.d.). User response to an SMS message sent to their contact number forms the third repudiation check. Two out of band validation steps greatly reduces the likelihood of spoofing attacks with little effort required of a legitimate patient establishing

their identify with the ASMIS application. This registration approach meets both patient-centric guiding principles and security requirement.

Patient database security permissions are restricted to the dedicated account used by business logic application functions and the database commands needed for those functions (OWASP Foundation, 2021). Connection credentials used by an application entity must be instantiated at runtime, not stored in code (Engel, 2020). These measures minimize the consequences of an attacker gaining access to the business logic server, -- STRIDE threat category Elevation of Privilege --, then making a direct patient connection to retrieve all records.

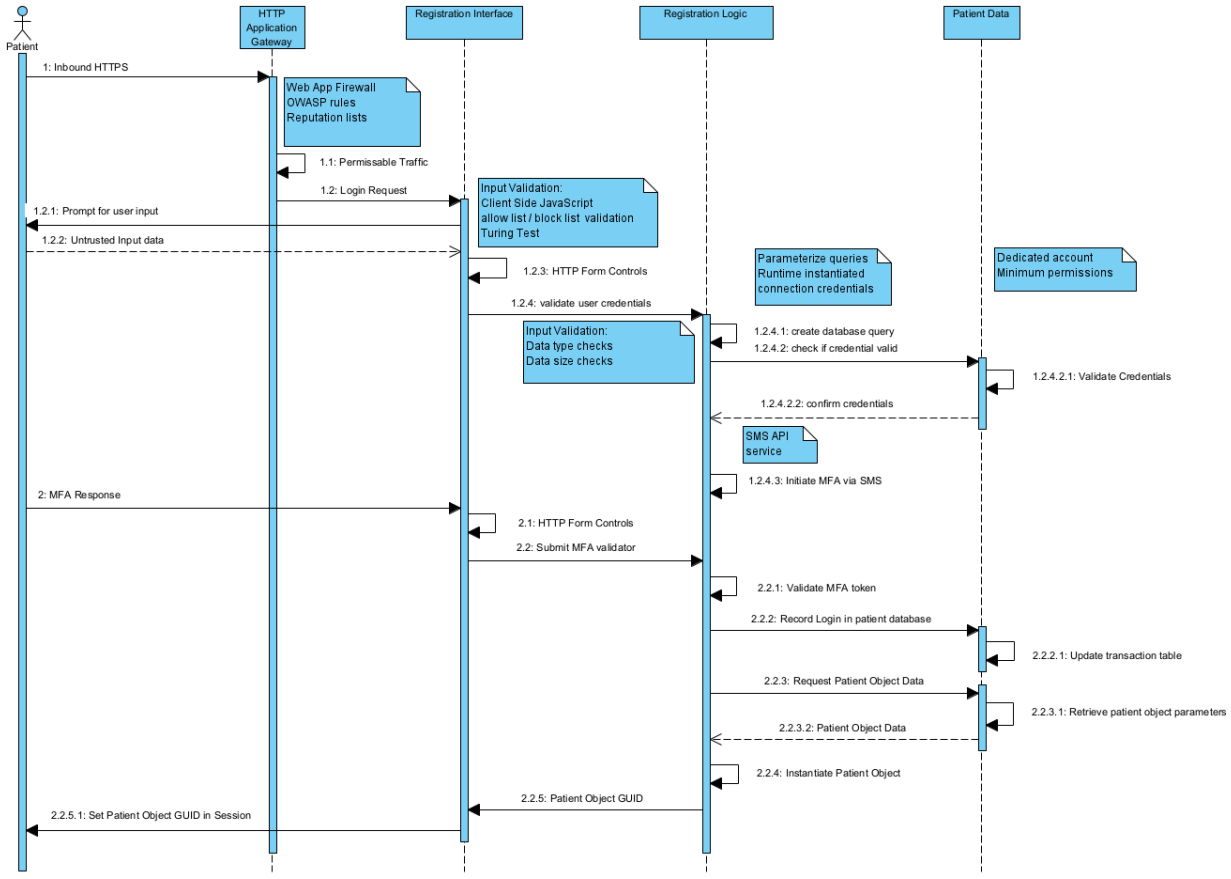

Figure 6 ASMIS Patient Authentication (negative responses tests omitted)

User interfaces for appointment request, selection, and change use cases will be protected by multi-factor authentication (MFA) because MFA reduces account compromise likelihood by more than 90% (Thomas & Moscicki, 2019). MFA requires safeguards to prevent nuisance prompts to registered patients being generated, avoiding negative patient perceptions about ASMIS. STRIDE Spoofing and Denial of Service concerns are addressed by initiating MFA prompts only after successful password validation. Credential stuffing attacks are mitigated using an optional Turing test such as Google's invisible reCAPTCHA (Google, 2021) to block suspicious login attempts without prompting legitimate users who simply mistyped their password.

All WAF and input validation protection mechanisms created for the registration interface will remain in place for the appointment request, select, and change use cases; one additional input validation is required for authenticated users. A patient's browser, unknowingly infected with malware, could expose confidential information, (STRIDE Information Disclosure). A globally unique identifier (GUID), created when an authenticated user object (Fig. 7) is instantiated, is used to maintain HTTP state without exposing the NHS number or ASMIS patient identifier.

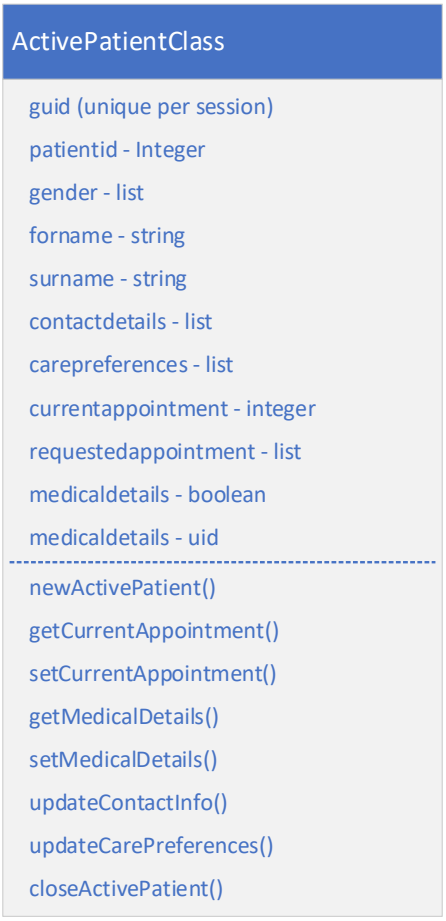

Figure 7 HTTP state management object

Patient input for managing appointments and symptom information are brokered through the authenticated user's unique instantiation of the ActivePatient class. Updates to each object are performed through method calls enabling additional data validation measures and error handling. Data retrieved from the object, rather than HTML application forms, will be used for patient database updates.

The final trust boundary is STRIDE Information Disclosure threats from internal attackers. Administrative controls will be required to determine whether patient record access was authorized (Adler, 2019) since employees and consultants must view patient data through ASMIS. IT administrative access risks can be

mitigated through products like transparent data encryption (TDE) (Oracle, 2021; Microsoft, 2021) to protect data at rest.

Conclusion:

Technology implementations provide both opportunities and inherent risks, justifying measured management decisions. With appropriate cyber security controls in place, the ASMIS application can meet Queens' patient-centric business objectives and risk tolerance. A conceptual architecture has been included (FIG. 8) to facilitate additional detailed analysis required for a comprehensive solution design. Additional risk assessment of the final solution design and penetration testing (National Cyber Security Center, n.d.) of the initial implementation are recommended to ensure effective mitigations are in place.

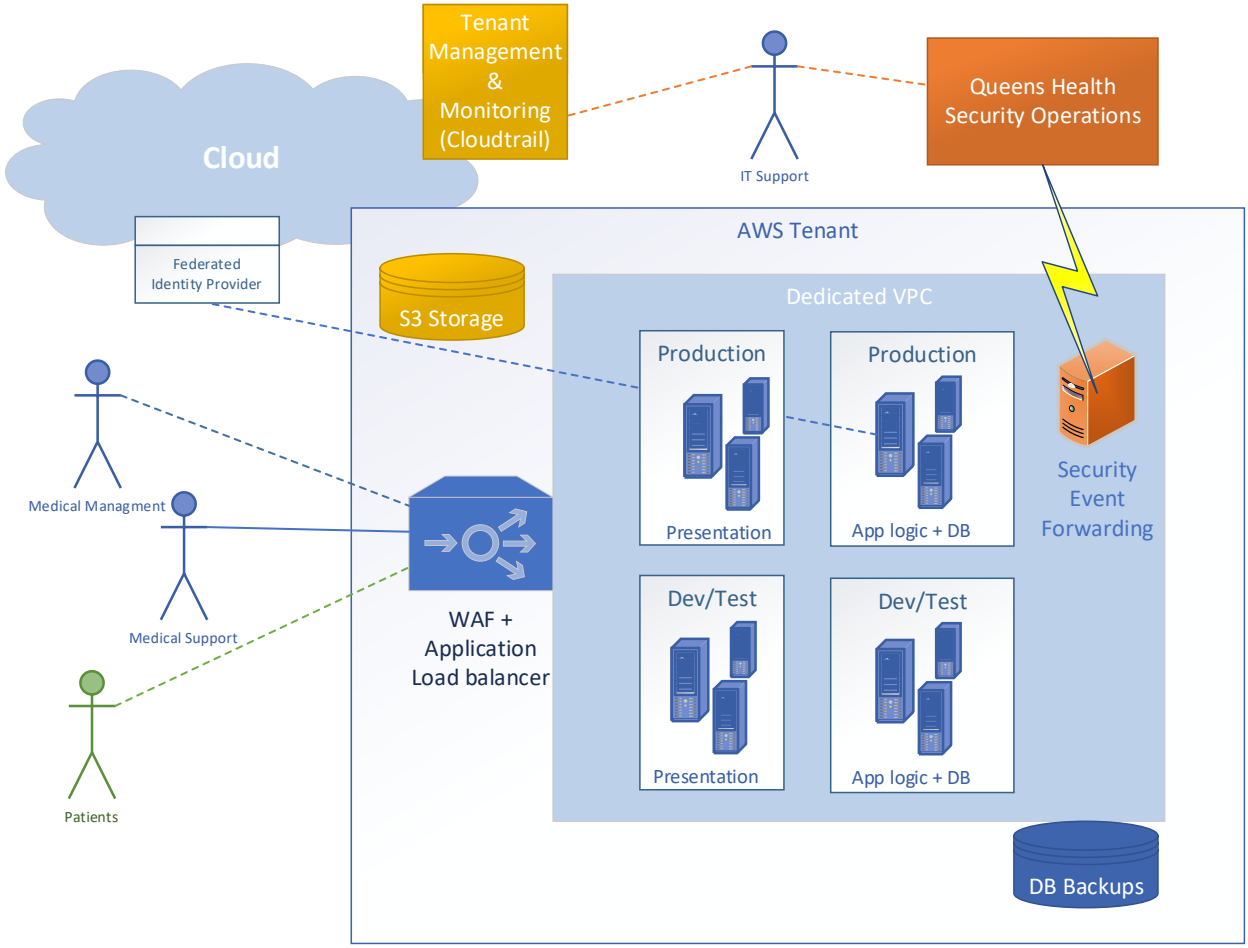

Figure 8 ASMIS Contextual Architecture

References

Adler, E. L. (2019) Practices risk hefty fines when employees snoop in EHRs. Available from: https://www.physicianspractice.com/view/practices-risk-hefty-fines-when-employees-snoop-ehrs [Accessed 3 July 2021].

Amazon Web Services. (2021) AWS WAF. Available from: https://docs.aws.amazon.com/waf/latest/developerguide/waf-chapter.html [Accessed 4 July 2021].

Canadian Centre for Cyber Security. (2020) How to Protect Your Organization From Insider Threats (ITSAP.10.003). Available from: https://cyber.gc.ca/en/guidance/how-protect-your-organization-insider-threats-itsap10003-0 [Accessed 2 July 2021].

Engel, D. (2020) Connection strings and configuration files. Available from: https://docs.microsoft.com/en-us/sql/connect/ado-net/connection-strings-and-configuration-files [Accessed 3 July 2021].

Fix, G. M. et al. (2018) Patient-centred care is a way of doing things: How healthcare employees conceptualize patient-centred care. *Health expectations : an international journal of public participation in health care and health policy* 21(1): 300-307. DOI:https://doi.org/10.1111/hex.12615

Froehle, C. M. & Magazine, M. J. (2013) 'Improving Scheduling and Flow in Complex Outpatient Clinics', in: Denton, B. (eds) *Handbook of Healthcare Operations Management. International Series in Operations Research & Management Science*. New York: Springer. 229-250.

GDPR.EU. (2021) What are the GDPR fines?. Available from: https://gdpr.eu/fines/ [Accessed 2 July 2021].

Georgiou, D. & Lambrinoudakis, C. (2021) Data Protection Impact Assessment (DPIA) for Cloud-Based Health Organizations. *Future Internet* 13(3): 66. DOI: https://doi.org/10.3390/fi13030066

Google. (2021) Choosing the type of reCAPTCHA. Available from: https://developers.google.com/recaptcha/docs/versions [Accessed 3 July 2021].

Howard, M. & LeBlanc, D. (2002) *Writing Secure Code.* 2nd ed. Redmond: Microsoft Press.

IBM. (2019) Patient-centric healthcare: It's time for a new operating model. Available from: https://www.ibm.com/blogs/services/2019/03/14/patient-centric-healthcare-its-time-for-a-new-operating-model/ [Accessed 1 July 2021].

Information Commisioner's Office. (2020) Information rights at the end of the transitions period Frequently Asked Questions Available from: https://ico.org.uk/media/for-

organisations/documents/brexit/2617110/information-rights-and-brexit-faqs-v2_3.pdf [Accessed 2 July 2021].

Lane, S. j., Heddle, N. M., Arnold, E. & Walker, I. (2006) A review of randomized controlled trials comparing the effectiveness of hand held computers with paper methods for data collection. *BMC Medical Informatics and Decision Making* 6(1): 23. DOI:https://doi.org/10.1186/1472-6947-6-23

Marhefka, K. M. (2020) *The Impact of Digital Self-Scheduling on No-Show Event Rates in Outpatient Clinics.* Doctoral thesis, Walden University.

McDerrmott, J. & Fox, C. (1999) 'Using abuse case models for security requirements analysis', 15th Annual *Computer Security Applications Conference*. Phoenix,AZ, 6-10 December. Los Alamitos: IEEE Computer Society. 55-64.

Microsoft. (2021) Transparent Data Encryption. Available from: https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/transparent-data-encryption [Accessed 3 July 2021].

National Cyber Security Center. (n.d.)Penatration Testing. Available from: https://www.ncsc.gov.uk/guidance/penetration-testing [Accessed 5 July 2021].

NHS Digitial. (n.d.) Personal Demographics Service - FHIR API. Available from: https://digital.nhs.uk/developer/api-catalogue/personal-demographics-service-fhir [Accessed 3 July 2021].

Offutt, J., Wu, Y., Huang, D. & Huang, H. (2004) 'Bypass testing of Web applications', *15th International Symposium on Software Reliability Engineering*. Saint-Malo,France, 2-5 November. Los Alamitos: IEEE Computer Society. 187-197.

Oracle. (2021) Frequently Asked Questions TDE. Available from: https://www.oracle.com/database/technologies/faq-tde.html [Accessed 3 July 2021].

Oswaldo, O., Dillig, I. & Lin, C. (2015) 'Detecting and Exploiting Second Order Denial-of-Service Vulnerabilities in Web Applications', *22nd ACM SIGSAC Conference on Computer and Communications Security*. Denver, Colorado, 12-16 October. New York: Association for Computing Machinery. 616-628.

OWASP Foundation. (2021) Database Security Cheat Sheet. Available from: https://cheatsheetseries.owasp.org/cheatsheets/Database_Security_Cheat_Sheet.html [Accessed 3 July 2021].

OWASP Foundation. (2020) Query Parameterization Cheat Sheet. Available from: https://cheatsheetseries.owasp.org/cheatsheets/Query_Parameterization_Cheat_Sheet.html [Accessed 2 July 2021].

OWASP Foundation. (n.d.) Business logic vulnerability. Available from: https://owasp.org/www-community/vulnerabilities/Business_logic_vulnerability [Accessed 4 July 2021].

OWASP Foundation. (2018) OWASP Proactive Controls. Available from: https://github.com/OWASP/www-project-proactive-controls/blob/master/v3/OWASP_Top_10_Proactive_Controls_V3.pdf [Accessed 2 July 2021].

Relatient. (n.d.) Why Patient Self-Scheduling: Healthcare Trends & Getting Started. Available from: https://www2.relatient.net/resources/why-patient-self-scheduling-healthcare-trends-getting-started/ [Accessed 30 June 2021].

Shostack, A. (2014) Threat Modeling designing for security. 1st ed. Indianapolis: John Wiley & Sons.

Tarandach, I. & Coles, M. J. (2020) Threat Modeling A practical Guide for Development Teams. 1st ed. Sebastopol: O'Reilly Media, Inc.

Thomas, K. & Moscicki, A. (2019) New research: How effective is basic account hygiene at preventing hijacking. Available from: https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html [Accessed 25 June 2021].

Trustwave. (2018) *2018 Trustwave Global Security Report,* Chicago: Trustwave.

University of Essex. (2021) Individual Essay. Available from: https://www.my-course.co.uk/mod/assign/view.php?id=495333 [Accessed 19 June 2021].

VENAFI. (n.d.) Common SSL Attack: SSL & TLS Key Vulnerability. Available from: https://www.venafi.com/education-center/ssl/common-ssl-attacks [Accessed 1 July 2021].

Verizon. (2021) DBIR 2021 Databreach Invetigations Report. Available from: https://www.verizon.com/business/resources/reports/dbir [Accessed 12 June 2021].

Zhao, P., Yoo, I., Lavoie, J., Lavoie, B. J. & Simoes, E. (2017) Web-Based Medical Appointment Systems: A Systematic Review. *Journal of Medical Internet Research* 19(4): e134. DOI: https://doi.org/10.2196/jmir.6747

Zhong, W. & Rezos. (n.d.) Code Injection. Available from: https://owasp.org/www-community/attacks/Code_Injection [Accessed 4 July 2021].