בס"ד

**1. שאלות על האפיון:**

1. מי המשתמשים באפילקציה? הפציינטים או עובדי קופ"ח?
2. אם האפליקציה היא עבור קופת חולים מסוימת ולא עבור משרד הבריאות, האם התראות הבידוד נשלחות רק לחברי הקופה?
3. אם האפליקציה היא עבור קופת חולים מסוימת ולא עבור משרד הבריאות, צריך לגשת לאיכוני הטלפון של כל אזרחי ישראל?
4. האם יש אפשרות לערוך קבוצה? למחוק קבוצה? לשלוף קבוצה? ולפי איזה שדות החיפוש יתבצע?
5. מהו המספר המקסימלי של אנשים שניתן לעדכן בבקשה בודדת? האם עלינו לשקול מגבלות כלשהן בצד השרת?
6. האם יש הגבלה למספר האנשים שניתן לכלול בבידוד קבוצתי? אם כן, מה הגבול וכיצד הוא נאכף?
7. כיצד יקבלו הפציינטים הודעה כאשר הם נוספו לבידוד קבוצתי? האם הם יקבלו התראה בטלפון או הודעה בכתב?
8. האם יש דרישות או תקנות ספציפיות שקופת החולים חייבת לעמוד בהן בעת יצירת בידודים קבוצתיים לחולים (למשל חוקי פרטיות החולה)?
9. מה הנוהל אם מישהו נחשב חולה והכניס אנשים לבידוד והתברר לבסוף שהוא לא חולה? כיצד יתעדכנו הפציינטים שהבידוד שלהם מבוטל?
10. מה הנוהל אם מישהו מקבוצת הבידוד מתגלה כחולה, האם זה מאריך את תקופת הבידוד לחברים בקבוצה? או אולי צריך לבדוק באילו מקומות נוספים הוא היה ולהוסיף אנשים נוספים לבידוד בהתאם.
11. מה קורה אם המשתמש מנסה לבחור מיקום מחוץ לאזור הגיאוגרפי הנתמך?
12. איך המערכת תוודא את אמינות המידע? האם ע"י הצלבת הנתונים של איכון הטלפון?
13. כיצד תטפל המערכת במקרים בהם משתמש הוא חלק ממספר בידודים קבוצתיים שחופפים בתאריך ו/או באנשים? לדוגמה, אם משתמש הוא חלק מבידוד קבוצתי משפחתי וגם חלק מבידוד קבוצתי למקום העבודה שלו, האם שני הבידודים יכולים להיות פעילים בו זמנית?
14. האם המערכת יכולה להתמודד עם בידודי קבוצות מרובים עבור אותה קבוצה של אנשים שיש להם תאריכי חשיפה או התאוששות שונים? לדוגמה, אם בן משפחה נחשף לנגיף בתאריך אחד, אך בן משפחה אחר נחשף במועד מאוחר יותר, האם ניתן ליצור שני בידודים קבוצתיים נפרדים?
15. האם יש עניינים משפטיים או שמירת פרטיות הקשורות לאיסוף ואחסון נתונים אלה? האם נקטנו בצעדים כדי להבטיח שהנתונים מאובטחים ונגישים רק לצוות מורשה?

**בהנחה שהפציינטים הם המשתמשים:**

1. כיצד תטפל המערכת במקרים שבהם מטופל יוצר בידוד קבוצתי אך חלק מהאנשים שהם מנסים להוסיף כבר יצרו בידוד קבוצתי משלהם?
2. האם מטופלים יוכלו להוסיף אנשים לבידוד קבוצתי אם אין להם אישור מאותם אנשים? אם לא, איך המערכת תאכוף זאת?
3. כיצד מטופלים יוכלו לראות את מצב הבידודים הקבוצתיים שלהם, ולראות מי צורף ומתי? האם מידע זה יהיה זמין בממשק המשתמש או באמצעות התראות?
4. האם יש דרך למטופלים לבטל בידוד קבוצתי לאחר יצירתו? אם כן, מה קורה לשאר האנשים שנוספו לבידוד הקבוצתי?
5. כיצד מטופלים יוכלו לערוך את הפרטים של בידוד קבוצתי, כגון תאריך החשיפה או ההחלמה, או רשימת האנשים שנוספו? האם יהיו הגבלות או הגבלות על התדירות שבה ניתן לשנות פרטים אלה?
6. מה קורה אם מטופל יוצר בידוד קבוצתי אבל שוכח להוסיף מישהו שנחשף גם הוא לנגיף? האם הם יכולים להוסיף את האדם הזה מאוחר יותר, או שהם יצטרכו ליצור בידוד קבוצתי חדש?
7. האם מטופלים יוכלו לראות היסטוריה של הבידודים הקבוצתיים שלהם, כולל בידודים קודמים שכבר הסתיימו? אם כן, כיצד יוצג מידע זה?

2**. מסמך בדיקות**

מקרי קצה לבדיקה:

1. בדיקה עם טווחי תאריכים לא חוקיים (תאריך התאוששות לפני תאריך החשיפה, תאריך חשיפה עתידי, תאריך התאוששות עתידי, או תאריך רחוק מדי בעבר.).
2. בדיקה עם קלט לא חוקי עבור מיקום (מיקום מחוץ לישראל, מיקום שאינו נגיש, מיקום שאינו נתמך ע"י גוגל מפס וכו').
3. בדיקה עם הכנסת קבוצה שכבר קיימת במאגר המידע.
4. בדיקה עם נתונים שגויים למערך האנשים שצריך לעדכן.
5. בדיקה עם מיקום באזור זמן שונה.
6. בדיקה עם תווים לא חוקיים(אימוג'י או תווים מיוחדים)
7. בדיקה עם השבתת שירותי המיקום במכשיר.
8. בדיקה עם שדות חסרים בבקשה.
9. בדיקה עם מספר רב של אנשים בבידוד הקבוצה.
10. בדיקות עם סוגים שונים של מיקומים (חנויות מכולת, בתי ספר וכו').
11. בדיקה עם סוגים שונים של מכשירים (נייד, שולחני, טאבלט).
12. בדיקה עם חיבורי אינטרנט איטיים.
13. בדיקה עם סוגים שונים של מפות (לוויין, שטח וכו').

בדיקות אבטחה:

1. בדיקת אימות והרשאה: בדוק את מנגנוני האימות וההרשאה כדי להבטיח שרק משתמשים מורשים יכולים לגשת למערכת ולבצע את הפעולות הדרושות. בדוק פגיעויות כגון סיסמאות חלשות ועמידות בפני מתקפות סייבר.
2. בדיקת אימות קלט: בדוק פגיעויות אימות קלט כגון הזרקת SQL, Scripting תקיפות XSS, ותקיפות זיוף בקשות (CSRF). ודא שהקלט מהמשתמשים מאומת כראוי כדי למנוע הזרקת קוד זדוני.
3. בדיקת הצפנת נתונים: בדוק את מנגנוני הצפנת הנתונים כדי להבטיח כי נתונים רגישים מוגנים כראוי בעת אחסון ושידור. בדוק פגיעויות כגון אלגוריתמי הצפנה חלשים, ניהול מפתחות הצפנה ודליפת נתונים.
4. בדיקת אבטחת API: בדוק את אבטחת ה-API כדי לוודא שה-API מאובטח .בדוק פגיעויות כגון הזרקת API, שיבוש פרמטרים והגבלת קצב API.
5. בדיקת אבטחת רשת: בדוק את אבטחת הרשת כדי לוודא שהמערכת אינה חשופה להתקפות רשת כגון התקפות מניעת שירות (DoS)והתקפות .MITM
6. בדיקת בקרת גישה: בדוק את מנגנוני בקרת הגישה כדי להבטיח שהגישה למשאבים מוגבלת כהלכה. בדוק פגיעויות כגון הגדרות ברירת מחדל לא מאובטחות, הרשאות קבצים לא מאובטחות ומעקף בקרת גישה.
7. בדיקת טיפול בשגיאות: בדוק את מנגנוני הטיפול בשגיאות כדי להבטיח שטעויות מטופלות היטב ואינן חושפות מידע רגיש. בדוק פגיעויות כגון מידע בהודעת שגיאה וכו'.
8. בדיקת ניהול תצורה: בדוק את מנגנוני ניהול התצורה כדי לוודא שהמערכת מוגדרת כהלכה ואינה מכילה הגדרות לא מאובטחות. בדוק פגיעויות כגון סיסמאות ברירת מחדל, יציאות פתוחות ופרוטוקולים לא מאובטחים.
9. בדיקת לוגיקה עסקית: בדוק את ההיגיון העסקי של המערכת כדי לוודא שהיא פועלת כמצופה ואינה מכילה נקודות תורפה לוגיות שעלולות להיות מנוצלות על ידי תוקפים.

בדיקת אינטגרציה:

1. בדוק את ההתממשקות של הבקשה בצד השרת ליצירת בידוד קבוצתי עם ה-API של מפות Google כדי להבטיח שנתוני המיקום מאוחזרים ומאוחסנים במדויק.
2. בדוק את איכוני הטלפון כדי לוודא שהאנשים הנכונים מזוהים כזקוקים לעדכון.
3. בדוק את השילוב של ה-iframe של ממשק המשתמש עם הבקשה בצד השרת כדי להבטיח שהלחצן "צור בידוד קבוצה" שולח את הנתונים הנכונים ומפעיל את העיבוד בצד השרת.
4. בדוק את האינטגרציה של הבקשה בצד השרת עם מסד הנתונים כדי להבטיח שנתוני בידוד הקבוצה מאוחסנים כהלכה וניתנים לאחזור.
5. בדוק את האינטגרציה של בקשת צד השרת לעדכון מצב הבידוד עם מערכת ההתראות כדי לוודא שהאנשים הנכונים מקבלים הודעה ושההודעות נשלחות בזמן.
6. בדוק את השילוב של הבקשה בצד השרת עם כל תכונות או מודולים רלוונטיים אחרים במערכת, כגון מעקב אחר אנשי קשר או דיווח על תוצאות בדיקה, כדי להבטיח שכל הרכיבים פועלים יחד בצורה חלקה.

בדיקות חווית המשתמש:

1. בדיקת ממשק המשתמש: ודא שממשק המשתמש ידידותי וקל לשימוש.
2. בדיקת ביצועי המערכת: בדוק את זמן התגובה, זמן הטעינה והיציבות של המערכת תחת עומסים ותרחישי שימוש שונים. ודא שהמערכת מסוגלת להתמודד עם עומס המשתמש הצפוי.
3. בדיקת שימושיות המערכת: בדיקת קלות השימוש, האינטואיטיביות והניווט של המערכת. ודא שמשתמשים יכולים למצוא בקלות את מה שהם צריכים ולבצע את הפעולות הנדרשות.
4. בדיקת רספונסיביות המערכת: בדיקת תאימות המערכת לדפדפנים, מכשירים ומערכות הפעלה שונות. ודא שהמערכת פועלת כהלכה בכל הפלטפורמות הנתמכות.
5. בדיקת נגישות המערכת: בדיקת נגישות המערכת למשתמשים עם מוגבלויות. ודא שהמערכת תואמת לתקני נגישות ולהנחיות.
6. בדיקת לוקליזציה של המערכת: בדוק את תכונות הלוקליזציה של המערכת כדי לוודא שהיא תומכת במספר שפות ותרבויות. ודא שהמערכת מציגה את השפה והניואנסים התרבותיים הנכונים.
7. בדיקת טיפול בשגיאות של המערכת: בדיקת מנגנוני הטיפול בשגיאות והשחזור של המערכת. ודא שהודעות השגיאה ברורות ואינפורמטיביות, והמערכת מספקת הדרכה מתאימה למשתמשים.
8. בדיקת תיעוד המערכת: ודא שתיעוד המערכת מדויק, מלא וקל להבנה. ודא שהמדריך למשתמש, קבצי העזרה והשאלות הנפוצות מספקים את המידע הנדרש למשתמשים.

בדיקות עומס:

1. בדוק את המספר המרבי של משתמשים בו-זמנית שהמערכת יכולה להתמודד איתם מבלי לקרוס.
2. בדוק את זמן התגובה של המערכת תחת עומס רב.
3. בדוק את יכולת המערכת להתאושש מקריסה הנגרמת מעומס רב.
4. בדוק את יכולת המערכת לטפל בשאילתות מורכבות בעומס רב.
5. בדוק את יכולת המערכת להתמודד עם מערכי נתונים גדולים תחת עומס רב.
6. בדוק את יכולת המערכת לטפל במספר בקשות בו זמנית.
7. בדוק את יכולת המערכת להתמודד עם אימות והרשאה של משתמשים בעומס רב.
8. בדוק את יכולת המערכת לשמור על עקביות נתונים תחת עומס רב.