의료 시뮬레이터 보안 설계 및 적용 문서

# 1. 환경 변수 (.env) 구성

• 모든 API Key, Firebase 키, Mongo URI 등은 `.env` 파일에 저장  
• 예시:  
 REACT\_APP\_API\_URL=https://api.medicalsimulator.com  
 MONGO\_URI=mongodb+srv://... (서버 측)  
• 배포 시 .env는 `.gitignore`에 반드시 포함

# 2. HTTPS 인증서 구성 (Self-signed / Production)

• 로컬 테스트용 self-signed SSL 인증서 생성:  
 openssl req -nodes -new -x509 -keyout server.key -out server.cert  
• Express 서버에 적용:  
 const https = require('https');  
 const options = { key: fs.readFileSync('server.key'), cert: fs.readFileSync('server.cert') };  
 https.createServer(options, app).listen(443);

# 3. Content-Security-Policy (CSP) 설정

• HTML 또는 서버 응답 헤더에 다음 포함:  
 Content-Security-Policy: default-src 'self'; script-src 'self'; style-src 'self' 'unsafe-inline';  
• 외부 리소스를 제한하여 XSS, 데이터 유출 방지

# 4. 보안 HTTP 헤더 설정 (Helmet 사용)

• Express 서버에서 helmet 미들웨어 사용:  
 const helmet = require('helmet');  
 app.use(helmet());  
• X-XSS-Protection, X-Content-Type-Options 등 보안 헤더 자동 적용

# 5. 클라이언트 코드 난독화 및 디버깅 방지

• webpack-obfuscator를 통해 난독화 적용  
• 콘솔 접근, F12, DevTools 감지 차단  
• Web Speech API, Socket, Firebase 인증 모두 암호화 채널 상에서 동작