
약국 개인정보보호 자율점검 가이드

2015. 9.

대 한 약 사 회

- 목 차 -

1. 자율점검지원시스템 접속	3
2. 자율점검서비스 신청서 작성	9
3. 자율점검 항목별 작성가이드	11
4. 기타 주요 점검사항	36

✓ 개인정보보호 자율점검의 개요

요양기관(약국)에서 자율적으로 개인정보 관리 실태를 점검할 수 있도록 개인정보보호법에서 준수해야 할 내용을 점검항목(체크리스트)화 하여 심사평가원에서 운영하는 요양기관업무포털 내 구축한 “자율점검지원시스템”을 통해 실시

※ 개인정보보호법에 대한 이해와 관리실태 점검을 통하여 미비사항을 보완하는 과정으로 약국 외 타인을 통한 대리점검은 자제해 주시기
바라며 일부 항목의 기술적인 사항은 프로그램 개발 업체 또는 A/S업체의 지원을 받아 작성하여 주시기 바랍니다.

✓ 자율점검 절차

- ① (약국) 자율점검지원시스템 접속
- ② (약국) 자율점검서비스 신청(기초현황 작성·제출)
- ③ (심사평가원) 접수·승인(심사평가원)
- ④ (약국) 자율점검 실시(총 40개 점검항목)
- ⑤ (약국) 자율점검 완료
- ⑥ (심사평가원) 자율점검 결과 검토
- ⑦ (약국) 보완조치 이행 : 6개월 내

1. 자율점검지원시스템 접속



① 인터넷 익스플로어 실행

②-1 요양기관업무포털 접속 방법

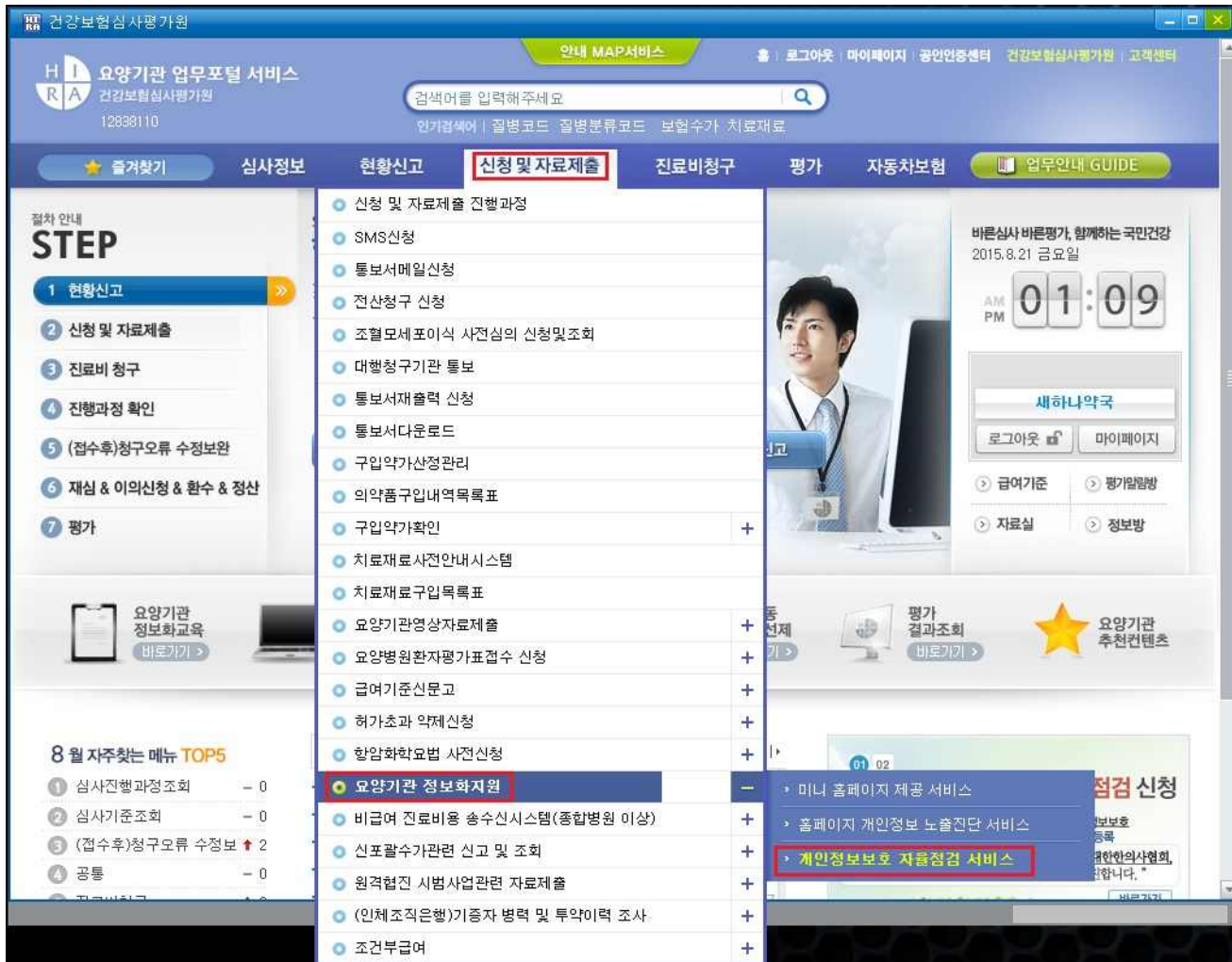
심사평가원(<http://www.hira.or.kr>) 접속 후
하단 배너에서 “요양기관업무포털”클릭



②-2 요양기관업무포털 접속 방법
 인터넷 주소창에 <http://biz.hira.or.kr>



- ③ 로그인: 공단에서 발급받은 약국 공인인증서 선택, 인증서 비밀번호 입력 후 확인
- ↳ 심사평가원 최초 로그인시 공인인증센터에서 공인인증서 등록 필요
- ↳ 심사평가원 홈페이지 (우측)상단 공인인증센터 클릭
- ↳ 공인인증서등록 메뉴 선택
- ↳ 요양기관, 보장기관 공인인증서등록 클릭



③ 개인정보보호 자율점검서비스로 이동

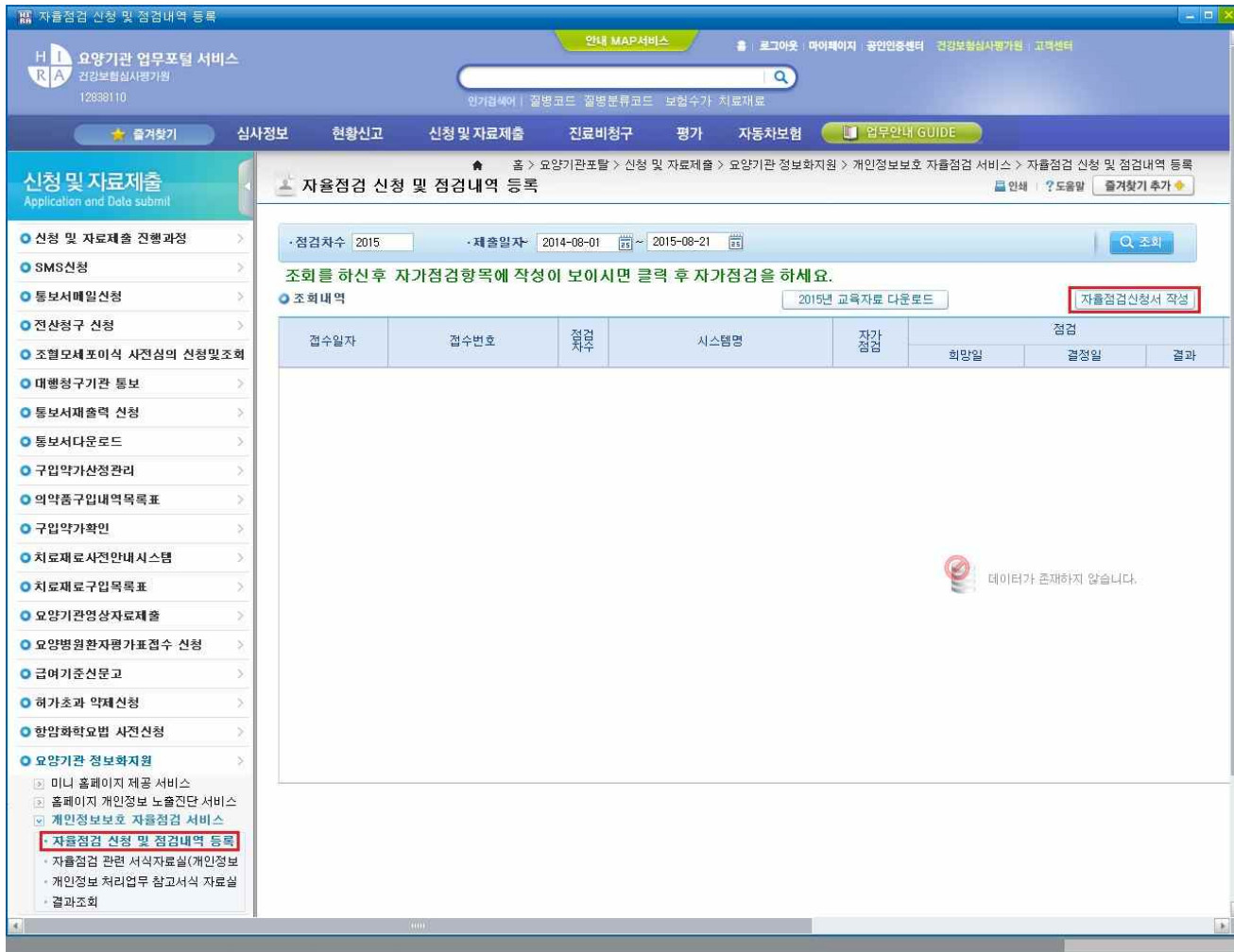
▷ 신청 및 자료제출

▷ 요양기관정보화지원

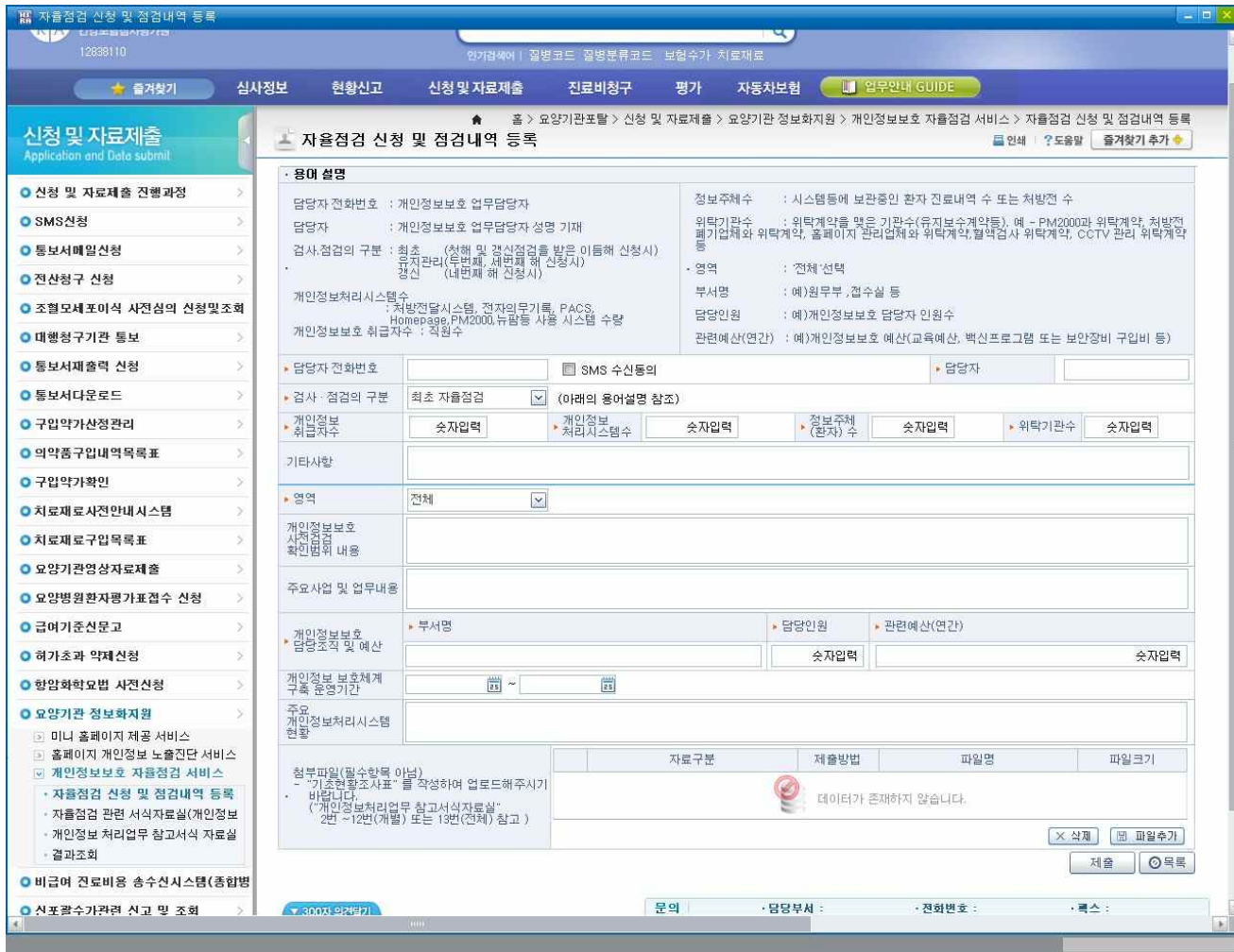
▷ 개인정보보호자율점검

▷ 자율점검 신청 및 점검내역 등록

▷ 자율점검 신청서 작성



④-1 자율점검신청서 작성



④-2 자율점검신청서 작성

<자율점검 신청 및 점검내역 등록>

II. 자율점검서비스 신청서 작성

✓ 자율점검 신청서 작성

항 목 명	설명	가이드
담당자 전화번호	법에 의거 약국은 개인정보책임자 및 개인정보담당자를 1인 이상 반드시 지정하여야 함	1인 약국은 약국장이 개인정보책임자/담당자/취급자가 되며, 2인 이상의 약국에서는 분담하여 지정할 수 있음
담당자		
검사·점검의 구분	자율점검 실시 횟수	“최초” 선택
개인정보 파일수	보관중인 개인정보 파일수로 약국에서 사용하는	청구프로그램에 저장된 조제기록부의 수를 의미
개인정보처리시스템수	개인정보를 처리하는 전산시스템	PC에 설치된 PM2000 등 청구프로그램 수를 의미함 예) PC 2대중 1대만 설치: 1, 서버에 데이터를 저장하고 클라이언트 PC에서 접속하여 사용하는 경우는 1
정보주체수	개인정보의 주체	약국에서 관리하는 고객(환자)의 수 청구프로그램에 저장된 고객(환자)수 기재
위탁기관수	개인정보처리 제3자 위탁계약 대상(업체)의 수	약국에서 위탁계약이 필요한 경우는 청구프로그램업체, 처방전 보관/폐기업체, CCTV 관리업체 등을 말함
개인정보보호 담당조직 및 예산	1인 약국의 경우 별도의 조직구성이나 예산계획이 없기 때문에 담당조직은 공란, 예산은 V3 등 백신/보안프로그램 갱신(유지) 비용 기재	
부서명	약국내 전담부서 등 조직구성이 있을 경우에만 기재	
담당인원	1인 약국의 경우 약국장이 개인정보책임자 및 담당자가 되므로 1로 표기하고 1인 이상 약국은 근무약사 또는 직원을 개인정보담당자로 지정하는 경우 해당인원 기재	
예산	개인정보보호를 위해 지출된 비용으로 정품백신 구입, 갱신 및 별도 보안프로그램 도입 비용, 처방전 보관을 위해 지출된 금액을 기재	
기초현황조사표 : 표준 샘플서식 다운로드 후 표시항목을 약국에 맞게 수정 후 첨부		

✓ 자율점검 신청서 접수·승인

심사평가원에서 승인하며 2~3일 소요됨, 처리 상태에서 확인이 가능하며 “승인”으로 표시되면 다음 단계 “자율점검 실시”로 이동할 수 있음

✓ 자율점검

약국에서 점검하는 항목은 총 44개 항목으로 해당 항목별로 점검결과를 작성함

점검은 점검항목 전체를 단번에 작성하지 않아도 되며, 저장 후 다시 접속하여 최근 점검항목 이후 항목부터 계속 작성할 수 있음

Ⅲ. 자율점검 항목별 작성가이드

이행여부에 따른 '운영현황' '관련문서 제목' '첨부파일' 작성 요령

이행여부	운영현황	첨부파일	<ul style="list-style-type: none"> ■ 이행여부가 [양호] [개선필요]인 경우 제시된 '운영해당' 내용을 참고하여 기재하고 해당 파일을 첨부하시기 바랍니다. ■ 이행여부가 [취약] [해당사항 없음]인 경우 '운영현황' 미기재 및 '첨부파일'은 없습니다. ■ 첨부파일은 표준 서식파일을 다운받아 약국에 맞게 일부내용을 수정한 후 첨부하시기 바랍니다.
[양호]	작성	첨부	
[개선필요]	작성	X	
[취약]	X	X	
[해당사항 없음]	X	X	

약국 유형별 점검항목 정리

*각 항목 우측상단 번호 참조

약국 유형		제외항목(이행여부를 [해당사항 없음] 선택)
1 ~ 4인 약국	홈페이지(또는 서면) 회원가입 X	13개 항목(1, 2, 3, 4, 11, 12, 13, 14, 15, 16, 26, 27, 37) 제외
1 ~ 4인 약국	홈페이지(또는 서면) 회원가입 ○	3개 항목(26, 27, 37) 제외
5인 이상 약국	홈페이지(또는 서면) 회원가입 X	10개 항목(1, 2, 3, 4, 11, 12, 13, 14, 15, 16) 제외
5인 이상 약국	홈페이지(또는 서면) 회원가입 ○	

* CCTV 미설치 약국 : 4개 항목(17, 18, 19, 20) 제외

* 1인 약국만 제외 : 24번 항목

1.1.1	온·오프라인 회원 가입 시 동의는 받고 있는가?		1	
설명	<p>회원가입이 필요한 홈페이지를 운영하거나 별도의 서비스(홍보, 마케팅, 상담 등) 제공을 목적으로 고객(환자)의 개인정보를 수집·이용(서면)하는 경우 필수 고지항목을 고객(환자)에게 알려주고 동의를 받고 있는지 확인</p> <p>※ 필수 고지항목</p> <ul style="list-style-type: none"> ▶ 개인정보의 수집/이용 목적 ▶ 수집하려는 개인정보의 항목 ▶ 개인정보의 보유 및 이용기간 ▶ 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 내용 			
가이드	이행여부	운영현황		첨부파일
	양호	필수 고지항목을 모두 포함하여 동의를 받고 있음		(서면) 개인정보 수집·동의서 (홈페이지) 홈페이지 주소
	개선필요	필수 고지항목의 일부가 누락되어 동의를 받고 있음		
	취약	필수 고지항목 누락, 회원가입 동의 누락		
	해당사항 없음	홈페이지 미운영 또는 별도의 서비스(홍보, 상담, 마케팅 등) 제공을 위한 회원가입 사실이 없음		
1.1.2	각종 게시판, 기타 개인정보 수집 시 동의를 받고 있는가?		2	
설명	<p>홈페이지를 운영하는 약국에서 홈페이지 내 게시판(건의사항, 상담, 자유게시판 등)을 통해 개인정보를 수집하는 경우, 개인정보 수집·이용에 관한 사항을 알려주고 동의를 받는지 확인</p> <p>※ 필수 고지항목</p>			

	<ul style="list-style-type: none"> ▶ 개인정보의 수집/이용 목적 ▶ 수집하려는 개인정보의 항목 ▶ 개인정보의 보유 및 이용기간 ▶ 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 내용 		
가이드	이행여부	운영현황	첨부파일
	양호	필수 고지항목을 모두 포함하여 동의를 받고 있음	(서면) 개인정보 수집·동의서 (홈페이지) 홈페이지 주소
	개선필요	필수 고지항목의 일부가 누락되어 동의를 받고 있음	
	취약	필수 고지항목 누락, 회원가입 동의 누락	
	해당사항 없음	홈페이지 미운영 또는 별도의 서비스(홍보, 상담, 마케팅 등) 제공을 위한 회원가입 사실이 없음	

1.2.1	목적에 필요한 최소한의 개인정보를 수집하고 있는가?		3
설명	<p>회원이 가입이 필요한 홈페이지를 운영하거나 별도의 서비스(홍보, 마케팅, 상담 등) 제공을 목적으로 고객(환자)의 개인정보를 수집·이용하는 경우 개인정보 수집 목적을 달성하기 위해 반드시 수집해야 하는 최소한의 정보(필수정보)만 수집하고 있는지 확인 예) 의약품 및 건강 상담을 목적으로 개인정보를 수집할 때 상담목적과 관련 없는 개인정보를 수집하는 경우</p> <p>※ 조제, 복약지도와 관련한 업무 처리 시 고객(환자)의 연락처 수집은 별도의 동의가 필요하지 않음</p>		
가이드	이행여부	운영현황	첨부파일
	양호	최소한의 개인정보만 수집하고 있음	(서면) 개인정보 수집·동의서 (홈페이지) 홈페이지 주소

	개선필요	목적에 불필요한 개인정보를 일부 수집하고 있음	
	취약	목적에 불필요한 개인정보를 다수 수집하고 있음	
	해당사항 없음	홈페이지 미운영 또는 별도의 서비스(홍보, 상담, 마케팅 등) 제공을 위한 회원가입 사실이 없음	

1.2.2	최소한의 정보 외의 개인정보 수집에 대한 미동의를 이유로 재화 또는 서비스 제공을 거부하고 있지 않은가?		4
설명	<p>회원이 가입이 필요한 홈페이지를 운영하거나 별도의 서비스(홍보, 마케팅, 상담 등) 제공을 목적으로 고객(환자)의 개인정보를 수집·이용하는 경우 개인정보 수집 목적을 달성하기 위해 반드시 수집해야 하는 최소한의 정보(필수정보)와 선택정보에 대하여 동의하지 않을 경우 회원가입 또는 기본적인 서비스 제공이 가능한지 확인</p> <p>예) 홈페이지 회원가입 시 선택정보임에도 불구하고 미동의시 회원가입이 되지 않는 경우</p>		
가이드	이행여부	운영현황	첨부파일
	양호	필수정보 외 선택정보 미동의시 회원가입 또는 서비스 제공	(서면) 개인정보 수집·동의서 (홈페이지) 홈페이지 주소
	취약	필수정보 외 선택정보 미동의시 회원가입 또는 서비스 제약	
	해당사항 없음	홈페이지 미운영 또는 별도의 서비스(홍보, 상담, 마케팅 등) 제공을 위한 회원가입 사실이 없음	

1.3.1	제3자에게 개인정보 제공 및 목적 외 이용 시 정보주체의 별도 동의를 받고 있는가?		5
설명	<p>개인정보를 제3자에게 제공할 때에는 원칙적으로는 고객(환자)의 동의를 받아야 하지만 ‘처방전 접수’, ‘요양급여비용 청구’, ‘약</p>		

<p>품 부작용 보고’, ‘응급환자 치료를 위한 응급의료기관의 요청 시’에는 고객(환자)의 동의 없이 제공이 가능함 일반 의료기관이나 보험회사 등에서 고객(환자)의 개인정보를 요청하는 경우에 별도 동의를 받고 제공하는지 확인 ※ 개인정보를 제3자에게 제공하는 경우 약국은 관리대장 기록·관리는 권고사항임</p>				
가이드	이행여부	운영현황		첨부파일
	양호	별도 동의가 필요한 경우 동의를 받고 제3자에 제공		개인정보 제3자 제공 동의서
	취약	별도 동의가 필요한 경우 동의 없이 제3자에 제공		
	해당사항 없음	제3자 제공 사실이 없음		

1.4.2	개인정보 제공시 제공목적 범위 내 이용, 안전조치 실시, 목적 달성 후 파기 등을 요청하고 있는가?			6
설명	별도 동의가 필요하여 수집한 개인정보를 제3자에게 제공할 때 제공받는 자에게 ▲목적 범위 내 이용 ▲‘목적 달성 후 파기 ▲ 안전한 관리를 위한 안전조치 기준 준수 요청을 하고 있는지 확인			
가이드	이행여부	운영현황		첨부파일
	양호	개인정보 제3자 제공시 제공받는 자에게 안전조치를 요청하고 있음		제3자 제공시 안전조치 요청 문서
	취약	개인정보 제3자 제공시 제공받는 자에게 안전조치를 요청하지 않고 있음		
	해당사항 없음	제3자 제공 사실이 없음		

1.5.1	보유기간 경과, 처리목적(제공받는 경우 제공받은 목적) 달성 후 지체 없이 개인정보는 파기하고 관리대장을 작성하여 관리하고 있는가?			7
-------	---	--	--	---

설명	<p>보유기간이 경과하거나 처리 목적을 달성한 개인정보(처방전, 전산데이터(조제기록부, 청구정보), 백업데이터, 별도 수집한 개인정보)를 지체 없이(5일 이내) 파기하고 ‘개인정보 파기 관리대장’에 기록·관리하는 확인</p> <p>▶ 종이처방전 : 위탁업체에서 수거한 처방전을 파기한 후 ‘사실확인서’ 또는 ‘증빙(사진)자료’를 첨부하여 ‘개인정보 파기 관리대장’에 첨부하여 기록·관리</p> <p>▶ 전산데이터 : PM2000 / 유팜 등 약국관리프로그램에서 제공한 개인정보 파기 기능을 이용하여 파기</p> <p>※ 파기방법 : 보유기간이 경과한 처방전, 전산데이터의 파기는 일정범위의 기간을 설정하여 파기할 수 있으나, 동 사항을 개인정보처리방침에 명시하여야 함</p> <p style="padding-left: 40px;">(예 : 개인정보처리방침에 OO약국은 보유기간이 경과한 개인정보를 매6개월 단위로 파기하고 있음을 명시)</p> <p>※ 보유기간 : 처방전 2년(요양급여비용을 청구한 처방전은 3년), 요양급여청구정보 5년, 조제기록부 5년 보관</p>
----	---

	이행여부	운영현황	첨부파일
가이드	양호	보유기간이 경과한 개인정보를 지체 없이 파기하고 관리대장에 기록·관리하고 있음	사실 확인서, 파기사진 등 증빙자료 또는 개인정보 파기 관리대장
	개선필요	보유기간이 경과한 개인정보를 지체 없이 파기하고 있으나 관리대장 기록, 관리는 하지 않음	
	취약	보유기간이 경과한 개인정보를 지체 없이 파기하지 않고 관리대장 기록, 관리도 하지 않음	
	해당사항 없음	파기할 개인정보가 없음	

1.5.2	개인정보 파기 시 복구 또는 재생되지 않도록 조치하고 있는가?	8
-------	------------------------------------	---

설명	보유기간이 경과하거나 처리 목적을 달성한 개인정보(처방전, 전산데이터(조제기록부, 청구정보), 백업데이터, 별도 수집한 개인 정보) 파기 시 복원이 불가능한 방법으로 영구 삭제하고 있는지 확인 ※ 종이처방전 파기 위탁업체에 파기방법(천공, 용해, 소각, 파쇄) 확인, 전산데이터의 경우는 외장하드 등 별도의 저장매체에 백업한 데이터만 복원이 불가능하도록 로우레벨포맷의 방법으로 파기		
가이드	이행여부	운영현황	첨부파일
	양호	개인정보 파기 시 재생 또는 복구가 불가능한 방법으로 파기하고 있음	사실 확인서, 파기사진 등 증빙자료 또는 개인정보 파기 관리대장
	취약	개인정보 파기 시 재생 또는 복구가 불가능한 방법으로 파기하지 않고 있음	

1.5.3	임시파일 및 출력자료 등은 목적달성 후 즉시 파기하고 있는가?		9
설명	업무수행 상 보존의 필요성 없이 임시로 생성한 개인정보가 포함된 파일(한글문서, 텍스트, 엑셀문서 등) 또는 출력물을 사용 후 즉시 파기하고 있는지 확인		
가이드	이행여부	운영현황	첨부파일
	양호	임시파일 또는 출력물은 목적달성(사용) 후 즉시 파기하고 있음	개인정보 파기 방법·절차가 수록된 개인정보처리방침 또는 내부관리계획
	취약	임시파일 또는 출력물은 목적달성(사용) 후 즉시 파기하고 않고 있음	
	해당사항 없음	임시파일 또는 출력물을 사용하는 경우가 없음	

1.5.4	법령에 따라 보존할 경우 별도로 분리 보관하고 있는가?		10
설명	<p>개인정보 보유기간이 경과하거나 처리목적이 달성된 개인정보(처방전, 전산데이터(조제기록부, 청구정보), 백업데이터, 별도 수집한 개인정보)를 법령에 근거하여 개인정보의 전부 또는 일부를 계속 보유할 경우에 별도로 분리 보관하는지 확인</p> <p>※ 보유기간 : 처방전 2년(요양급여비용을 청구한 처방전은 3년), 요양급여청구정보 5년, 조제기록부 5년 보관</p>		
가이드	이행여부	운영현황	첨부파일
	양호	분리보관 하고 있음	계속 보유하는 개인정보 관리대장
	취약	분리보관 하지 않음	
	해당사항 없음	분리보관이 필요한 개인정보가 없거나 해당되는 경우가 없음	

1.6.1	최소 개인정보(필수정보)와 그 외의 개인정보(선택정보)를 구분하여 동의를 받고 있는가?		11
설명	<p>회원가입이 필요한 홈페이지를 운영하거나 별도의 서비스(홍보, 마케팅, 상담 등) 제공을 목적으로 고객(환자)의 개인정보를 수집·이용하는 경우 개인정보 수집 목적을 달성하기 위해 반드시 수집해야 하는 최소한의 정보(필수정보)외 선택정보를 구분하여 동의를 받고 있는 지 확인</p>		
가이드	이행여부	운영현황	첨부파일
	양호	개인정보 수집 시 필수정보와 선택정보를 구분하여 동의를 받고 있음	(서면) 개인정보 수집·동의서 (홈페이지) 홈페이지 주소

	개선필요	개인정보 수집 시 필수정보와 선택정보를 구분하지 않고 동의를 받고 있음
	취약	개인정보 수집 시 동의 절차가 없음
	해당사항 없음	홈페이지 미운영 또는 별도의 서비스(홍보, 상담, 마케팅 등) 제공을 위한 회원가입 사실이 없음

1.6.2	만14세 미만 아동의 개인정보를 수집하는 경우 법정대리인의 동의를 받고 있는가?		12
설명	회원가입이 필요한 홈페이지를 운영하거나 별도의 서비스(홍보, 마케팅, 상담 등) 제공을 목적으로 고객(환자)의 개인정보를 수집·이용하는 경우 만 14세 미만 아동의 개인정보는 법정대리인의 동의를 받고 있는지 확인		
가이드	이행여부	운영현황	첨부파일
	양호	만 14세 미만 아동의 개인정보 수집 시 법정대리인의 동의를 받고 있음	(서면) 개인정보 수집·동의서 (홈페이지) 홈페이지 주소
	취약	만 14세 미만 아동의 개인정보 수집 시 법정대리인의 동의를 받지 않음	
	해당사항 없음	홈페이지 미운영 또는 별도의 서비스(홍보, 상담, 마케팅 등) 제공을 위한 회원가입 사실이 없음	

1.6.3	홍보 권유에 활용하기 위한 정보와 그렇지 않은 정보를 구분하여 동의를 받고 있는가?		13
설명	고객(환자)에게 재화나 서비스를 홍보하거나 판매를 권유를 목적으로 홈페이지 또는 서면을 통해 고객(환자)의 개인정보를 수집·이용하는 경우 필수항목을 포함하여 고객(환자)이 명확하게 인지할 수 있도록 구분하여 동의를 받고 있는지 확인		

	※ 필수항목 ▶ 개인정보의 수집/이용 목적 ▶ 수집하려는 개인정보의 항목 ▶ 개인정보의 보유 및 이용기간 ▶ 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용		
가이드	이행여부	운영현황	첨부파일
	양호	필수항목을 포함하여 구분하여 동의를 받고 있음	(서면) 개인정보 수집·동의서 (홈페이지) 홈페이지 주소
	개선필요	필수항목을 누락하거나 구분하지 않고 동의를 받고 있음	
	취약	필수항목 누락 및 구분하지 않고 동의를 받지 않고 있음	
	해당사항 없음	홈페이지 미운영 또는 별도의 서비스(홍보, 상담, 마케팅 등) 제공을 위한 회원가입 사실이 없음	

2.1.1	사상, 정치, 건강 등 민감정보를 동의에 의한 수집 및 제공 시 개인정보 수집 동의와 별도로 구분하여 동의를 받고 있는가?		14
설명	회원가입이 필요한 홈페이지를 운영하거나 별도의 서비스(홍보, 마케팅, 상담 등) 제공을 목적으로 고객(환자)의 개인정보를 수집·이용하는 경우 민감정보(사상, 정치, 건강 등)는 구분하여 동의를 받고 있는지 확인		
가이드	이행여부	운영현황	첨부파일
	양호	구분하여 동의를 받고 있음	(서면) 개인정보 수집·동의서 (홈페이지) 홈페이지 주소

	개선필요	구분하지 않고 동의를 받고 있음	
	취약	동의절차가 없음	
	해당사항 없음	홈페이지 미운영 또는 별도의 서비스(홍보, 상담, 마케팅 등) 제공을 위한 회원가입 사실이 없거나 민감정보를 수집하지 않음	

2.2.1	고유식별정보의 수집 및 제공 시 개인정보 수집 동의와 별도로 구분하여 동의를 받고 있는가? (주민번호, 여권번호, 운전면허번호, 외국인등록번호)		15
설명	<p>처방전 수집을 제외한 별도의 서비스(홍보, 마케팅, 상담 등) 제공을 목적으로 고객(환자)의 개인정보를 수집·이용하는 경우 고유 식별정보(여권번호, 운전면허번호, 외국인 등록번호)에 대해 구분하여 동의를 받고 있는지 확인</p> <p>※ 고유식별정보 중 주민번호는 절대 수집금지 사항임</p>		
가이드	이행여부	운영현황	첨부파일
	양호	구분하여 동의를 받고 있음	(서면) 개인정보 수집·동의서 (홈페이지) 홈페이지 주소
	개선필요	구분하지 않고 동의를 받고 있음	
	취약	동의절차가 없음	
	해당사항 없음	홈페이지 미운영 또는 별도의 서비스(홍보, 상담, 마케팅 등) 제공을 위한 회원가입 사실이 없음	

2.2.2	주민등록번호를 제외한 회원가입 방법을 제공하고 있는 가?		16
설명	회원가입이 필요한 홈페이지를 운영하는 경우 회원 가입 시 주민등록번호를 사용하지 않는 방법을 제공하고 있는지 확인		

	(주민등록번호를 제외한 회원가입 방법 : I-PIN, 신용카드 인증, 공인인증서, 휴대폰 인증)		
가이드	이행여부	운영현황	첨부파일
	양호	주민등록번호를 제외한 000의 방법으로 회원가입 방법을 제공하고 있음	홈페이지 주소
	취약	주민등록번호를 이용하여 회원가입을 받고 있음	
	해당사항 없음	홈페이지 미운영	

2.3.1	영상정보처리기기 운영·관리방침을 수립하고 있는가?		17
설명	CCTV 설치·운영 시 ‘영상정보처리기기 운영·관리방침’을 마련하고 안내하고 있는지 확인 (개인정보처리방침에 포함하여 안내해도 됨)		
가이드	이행여부	운영현황	첨부파일
	양호	영상정보처리기기 운영·관리방침을 마련하고 안내하고 있음	영상정보처리기기 운영·관리방침
	취약	영상정보처리기기 운영·관리방침을 마련하고 있지 않거나 안내하지 않음	
	해당사항 없음	영상정보처리기기를 운영하지 않음	

2.3.2	영상정보처리기기를 설치한 장소에 정보주체가 인지할 수 있도록 필수 기재사항을 포함한 안내판을 설치하였는가?		18
설명	CCTV 설치·운영 시 약국 출입구 등에 고객(환자)이 확인할 수 있도록 안내판을 설치하고 있는지 확인 ※ CCTV안내판 필수항목 ▲ 설치목적 ▲ 장소 ▲ 촬영범위 ▲ 시간 ▲ 관리책임자 성명 ▲ 연락처		

가이드	이행여부	운영현황	첨부파일
	양호	필수항목을 모두 포함하여 CCTV안내판을 설치하고 있음	CCTV안내판 설치 사진
	개선필요	필수항목이 일부 누락되어 CCTV안내판을 설치하고 있음	
	취약	CCTV안내판 미설치	
	해당사항 없음	영상정보처리기기를 운영하지 않음	

2.3.3	개인영상정보에 대한 이용·제공·열람·파기 내역을 기록 관리하는가?		19
설명	약국장은 CCTV를 통해 녹화되는 고객(환자)의 개인영상정보의 ▲수집목적 외 이용 ▲제3자 제공 ▲파기 ▲열람요청에 대한 기록을 관리하고 있는지 확인		
가이드	이행여부	운영현황	첨부파일
	양호	개인영상정보를 기록·관리하고 있음	개인영상정보 관리대장
	취약	개인영상정보를 기록·관리하지 않음	
	해당사항 없음	영상정보처리기기를 운영하지 않음	

2.3.4	개인영상정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 안전성 확보조치를 하고 있는가?		20
설명	개인영상정보(CCTV 녹화 데이터)가 분실, 도난, 유출, 변조되지 않도록 안전하게 관리하고 있는지 확인 ※ 개인영상정보가 PC에 저장되는 경우 PC 보안조치와 개인영상정보에 대한 열람, 삭제 등 접근을 제한하며 개인영상정보를 별도의 물리적인 시설에 보관할 경우 잠금장치 등)		
가이드	이행여부	운영현황	첨부파일

	양호	개인영상정보에 대한 안전성 확보 조치를 취하고 있음	영상정보처리기기 운영·관리방침
	개선필요	개인영상정보에 대한 안전성 확보조치가 미흡함	
	취약	개인영상정보에 대한 안전성 확보 조치를 취하고 있지 않음	
	해당사항 없음	영상정보처리기기를 운영하지 않음	

2.4.1	위탁 계약 시 문서(계약서)에 의한 계약을 하였는가?		21
설명	<p>개인정보 처리업무를 위탁 시 필수항목이 포함된 계약서에 의해 계약하고 있는지 확인</p> <p>※ 약국에서의 개인정보 처리업무 위탁의 예</p> <ul style="list-style-type: none"> ▶ 처방전 보관/파기 ▶ 약국관리프로그램 사용(PM200 : 메인화면 / 도움말 또는 PM2000 간략매뉴얼 바로가기 / ‘개인정보처리 위탁계약서’ 출력) ▶ 약국관리프로그램 유지·보수(A/S) ▶ CCTV 위탁 관리 <p>※ 필수항목</p> <ul style="list-style-type: none"> ▶ 위탁업무 수행 목적외 개인정보 처리 금지에 관한 사항 ▶ 개인정보의 기술적·관리적 보호조치에 관한 사항 ▶ 위탁하는 업무의 목적 및 범위 ▶ 재 위탁 제한에 관한 사항 ▶ 접근제한 등 안전조치 ▶ 개인정보의 관리 현황 점검 등 감독에 관한 사항 ▶ 수탁자가 준수하여야 할 의무를 위반할 경우 손해배상 등에 관한 사항 		
가이드	이행여부	운영현황	첨부파일

	양호	위탁 계약 시 필수항목을 모두 포함하여 계약하고 있음	위탁계약서 첫 장 스캔 또는 촬영사진 첨부
	개선필요	위탁 계약 시 필수항목 중 일부를 누락하여 계약하고 있음	
	취약	위탁 계약서가 없음	
	해당사항 없음	위탁한 사실이 없음	

2.4.2	수탁업체에 대한 교육 및 처리현황 점검 등 관리 감독을 실시하고 있는가?		22
설명	개인정보 처리업무 위탁 시 수탁업체에 대한 교육 및 관리 감독을 하고 있는지 확인 ※ 약국이 수탁업체를 대상으로 교육은 현실적으로 어렵기 때문에 수탁업체의 개인정보보호교육 이수 증빙서류를 제출받아 보관하는 것으로 교육을 대신할 수 있으므로 수탁업체에 교육이수 증빙서류를 제출토록 함(PM2000 : 메인화면 우측하단 바로가기 서비스 중 교육이수증 클릭)		
가이드	이행여부	운영현황	첨부파일
	양호	수탁업체의 교육이수증을 보관하고 개인정보보호 관리현황을 점검하고 있음	교육결과(수탁업체로부터 제출받은 교육이수 증빙)
	취약	수탁업체의 교육이수 증빙서류 미보관 및 관리현황 미점검	
	해당사항 없음	위탁한 사실이 없음	

2.4.3	위탁에 관한 사실을 인터넷 홈페이지, 사보 등에 공개하고 있는가?		23
설명	약국에서의 개인정보 처리업무 위탁(청구프로그램 개발·유지·보수/처방전 폐기/CCTV관리 등)에 관한 사실을 개인정보처리방침에 포함하여 고객(환자)이 인지할 수 있도록 처방접수대 등에 비치하거나 홈페이지(운영약국만 해당)에 공개하고 있는지 확인		

	※개인정보처리방침 포함되는 위탁에 관한 필수사항 ▲ 위탁기관(업체)명 ▲ 위탁업무 내용 ▲ 위탁기간		
가이드	이행여부	운영현황	첨부파일
	양호	개인정보 처리 위탁 시 개인정보처리방침에 위탁에 관한 필수사항을 포함하여 공개하고 있음	개인정보처리방침
	개선필요	개인정보 처리 위탁 시 개인정보처리방침에 위탁에 관한 필수사항 중 일부가 누락되어 공개하고 있음	
	취약	개인정보처리방침에 위탁에 관한 사항이 누락되거나 미공개	
	해당사항 없음	위탁 사실이 없음	

2.5.1	개인정보취급자에 대한 보안서약서는 징구 하였는가? (1인 약국 해당사항 없음)		24
설명	약국장은 근무약사, 전산직원 등 약국 근무자에 대하여 보안서약서를 받아 관리하고 있는지 확인		
가이드	이행여부	운영현황	첨부파일
	양호	약국 근무자에 대해 보안서약서를 징구하고 있음	보안서약서
	취약	보안서약서를 징구하지 않음	
	해당사항 없음	1인 약국	

2.5.2	개인정보취급자 및 일반직원에 대한 정기적인 교육은 실시하였는가?	25
-------	-------------------------------------	----

설명	약국장은 약국 근무자에 대하여 매년 1회 이상 정기적으로 개인정보보호 교육을 실시하고 있는지 확인 ※ 약국 근무자에 대한 개인정보교육은 관련기관교육, 개인정보개인정보보호포탈(http://www.privacy.go.kr)을 통한 온라인 교육(배움터) 및 관련 문서자료를 다운받아 교육에 활용할 수 있음			
가이드	이행여부	운영현황		첨부파일
	양호	매년 정기적으로 교육을 실시하고 있음		교육 결과 참고자료(권고사항)
	취약	매년 정기적인 교육 미실시		
	해당사항 없음	1인 약국		

3.1.1	내부관리계획을 수립하여 시행하고 있는가?(상시근무인력이 5인 이상인 약국 해당)			26
설명	상시 근무인원이 5인 이상인 약국에서는 개인정보를 안전하게 처리하기 위하여 필수사항을 반영하여 ‘내부관리계획’을 수립하고 있는지 확인 ※ 내부관리계획 수립 시 필수 반영사항 <ul style="list-style-type: none"> ▶ 개인정보 보호책임자 지정에 관한 사항 ▶ 개인정보 보호책임자 및 개인정보 취급자의 역할 및 책임에 관한 사항 ▶ 개인정보의 안전성 확보에 관한 사항 ▶ 개인정보 취급자에 대한 교육에 관한 사항 ▶ 개인정보 처리업무를 위탁하는 경우 수탁자에 대한 관리·감독에 관한 사항 ▶ 그 밖에 개인정보 보호를 위하여 필요한 사항 			
가이드	이행여부	운영현황		첨부파일
	양호	필수 반영사항을 포함하여 내부관리계획을 수립하고 있음		내부관리계획서

	개선필요	내부관리계획을 수립하고 있으나 필수 반영사항 중 일부가 누락되었음
	취약	내부관리계획 미수립
	해당사항 없음	1인 ~ 4인 약국

3.1.2	연간 개인정보보호 교육계획이 수립되어 있는가? (상시근무인력이 5인 이상인 약국 해당)		27
설명	상시 근무인원이 5인 이상인 약국에서 ▲교육목적 ▲대상 ▲내용 ▲일정·방법 등이 포함된 개인정보보호 교육계획을 매년 마련하거나 내부관리계획에 포함하고 있는지 확인		
가이드	이행여부	운영현황	첨부파일
	양호	교육목적, 대상, 내용, 일정·방법 등의 내용을 포함하여 교육계획을 수립하고 있음	내부관리계획서
	취약	교육계획 미수립	
	해당사항 없음	1인 ~ 4인 약국	

3.2.3	안전한 비밀번호 작성규칙을 적용하고 있는가?		28
설명	<p>약국에서 개인정보처리시스템(PM2000, 유팜 등 약국관리프로그램) 및 PC 로그인 시 안전한 비밀번호를 설정하고 사용하는지 확인</p> <p>※ 안전한 비밀번호 작성 규칙</p> <ul style="list-style-type: none"> ▶ 비밀번호가 3가지 이상(문자, 숫자, 영문, 특수문자 등) 조합인 경우 8자리 ▶ 비밀번호가 2가지 이상(문자, 숫자, 영문, 특수문자 등) 조합인 경우 10자리 		

※ PC로그인 시 비밀번호 설정 : 윈도우즈 / 제어판 / 사용자 계정			
가이드	이행여부	운영현황	첨부파일
	양호	안전한 비밀번호 작성규칙을 적용하여 사용하고 있음	개인정보처리방침 또는 비밀번호 작성 규칙이 반영된 문서
	취약	PC 또는 약국관리프로그램 로그인 시 안전한 비밀번호 미적용	

3.3.2	컴퓨터(PC)에 저장된 개인정보는 별도로 암호화 하고 있는가?		29
설명	업무용 PC 또는 모바일기기에 주민등록번호가 포함된 문서파일(hwp, xls, txt) 등을 암호화하여 관리하고 있는지 확인 ※ 문서파일의 암호화는 문서편집기에서 제공하는 암호설정 기능(예 : 한글편집기 / 보안 / 문서암호설정)이나 보안프로그램 등에서 제공하는 파일 보안기능 활용		
가이드	이행여부	운영현황	첨부파일
	양호	암호화 하여 관리하고 있음	개인정보처리방침 또는 비밀번호 작성 규칙이 반영된 문서
	취약	암호화 하지 않고 있음	
	해당사항 없음	주민등록번호가 포함된 문서파일 등이 없음	

3.5.1	개인정보처리시스템에 백신프로그램 등 최신의 보안프로그램을 설치하여 관리하고 있는가?		30
설명	컴퓨터바이러스, 악성코드 등을 방지·치료할 수 있는 백신프로그램(V3, 노턴 안티바이러스) 또는 보안프로그램을 설치·운용하고 있는지 확인 ※ 백신프로그램		

- ▶ 약국(사업장)의 경우 개인에게 무료사용이 허가된 V3 Lite, 알약, 네이버백신 등의 무료백신은 사용할 수 없으며, 사업장용 정품 백신소프트웨어(유/무료)를 사용하여야 함(☞10인 이내 사업장용 무료백신소프트웨어 : MS Security Essential)
- ▶ 백신프로그램이 설치되지 않은 약국은 심사평가원 요양기관업무포털 접속시 자동으로 백신프로그램이 설치됨

※ 보안프로그램

- ▶ 약국 PC 보안관리 사항을 준수하거나, 보안 강화를 위해 별도의 유료 보안프로그램(팜시큐리티 등)을 도입할 수 있음

〈약국관리프로그램 사용약국의 PC 보안관리 사항〉	
<ul style="list-style-type: none"> ▲ ID 공유금지 및 접속권한부여 : 1인 1 ID를 사용하며, ID는 공유하지 말고 업무상 불필요한 직원은 고객관리프로그램에 접속하지 못하도록 관리 ▲ 약국관리프로그램에 로그인 비밀번호 설정 <ul style="list-style-type: none"> - 고객관리프로그램의 안전성 강화를 위해 비밀번호를 설정하고, 최소 6개월 주기로 비밀번호 변경 필요 - 비밀번호는 영어대문자, 소문자, 숫자, 특수문자를 조합하여 10자 이상으로 2종류 조합 설정하거나 8자 이상으로 3종류 조합 설정 ▲ PC에 바이러스 백신 설치 및 관리 <ul style="list-style-type: none"> - 악성코드 차단을 위한 바이러스 백신을 설치하고 자동 업데이트 기능을 설치하여 주기적으로 관리 ▲ PC에 방화벽 설정 및 관리 <ul style="list-style-type: none"> - 고객정보에 대한 불법적 접근을 차단하기 위해 PC방화벽 설정 필요 ▲ 비밀번호, 주민등록번호의 암호화 확인 <ul style="list-style-type: none"> - 약국관리프로그램 제공업체에 비밀번호, 주민등록번호가 암호화되어 전송 및 저장되는지 확인 및 관리 필요 	

	이행여부	운영현황	첨부파일
가이드	양호	백신프로그램 등 보안프로그램 설치·사용하고 있음	백신프로그램 또는

			보안프로그램 계약서
	취약	백신프로그램 등 보안프로그램을 사용하고 있지 않음	

3.5.2	보안프로그램을 정기적(일 1회 이상)으로 업데이트 하는가?		31
설명	백신소프트웨어 등 보안프로그램에 자동업데이트 기능을 설정하거나 일 1회 이상 업데이트를 통해 최신상태로 유지하고 있는지 확인 (해당 프로그램의 환경설정 또는 업데이트 설정에서 자동업데이트 기능을 설정하거나 수동업데이트)		
가이드	이행여부	운영현황	첨부파일
	양호	자동업데이트 기능을 설정하여 일 1회 이상 업데이트를 하고 있음	
	개선필요	가끔 수동으로 업데이트를 실시하고 있음	
	취약	업데이트를 전혀 하지 않음	

3.6.1	전산실, 자료보관실 등 물리적 보관 장소에 대한 출입통제 절차를 수립하여 운영하고 있는가?		32
설명	처방전, 개인정보처리시스템을 약국 내/외부 별도의 물리적 보관 장소에서 관리하는 경우, 보관 장소에 대한 출입 통제절차를 수립하여 운영하고 있는지 확인		
가이드	이행여부	운영현황	첨부파일
	양호	출입 통제절차를 수립하여 관리하고 있음	출입통제 관리대장, 출입통제 규정이 반영된 개인정보처리방침

			또는 내부관리계획서
	취약	출입 통제절차가 없음	
	해당사항 없음	물리적 보관 장소가 없음	

3.6.2	개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하고 있는가?		33
설명	처방전 보관 시 잠금장치가 있는 보관함에 보관하고 있는지 확인 (백업데이터를 외장하드 등에 저장하여 보관하는 경우도 동일함)		
가이드	이행여부	운영현황	첨부파일
	양호	개인정보를 잠금장치가 있는 안전한 장소(보관함)에 보관하고 있음	개인정보처리방침 또는 내부관리계획서
	취약	잠금장치 및 보관함에 보관하지 않음	

3.7.1	개인정보처리방침을 수립하고 있는가? (필수항목 8개 반드시 포함)		34
설명	개인정보를 처리하는 약국에서 개인정보처리방침(필수 8항목 포함)을 수립하고 있는지 확인 ※필수 8항목 ▶ 개인정보의 처리목적 ▶ 개인정보의 처리 및 보유기간 ▶ 개인정보의 제3자 제공에 관한 사항 ▶ 개인정보처리의 위탁에 관한 사항 ▶ 정보주체의 권리·의무 및 그 행사방법에 관한 사항		

	<ul style="list-style-type: none"> ▶ 처리하는 개인정보의 항목 ▶ 개인정보 파기에 관한 사항 ▶ 개인정보 안전성 확보조치에 관한 사항 ▶ 개인정보보호 책임자 지정 ▶ 개인정보 처리방침의 변경이력 		
가이드	이행여부	운영현황	첨부파일
	양호	필수 8항목을 포함하여 개인정보처리방침 수립하고 있음	개인정보처리방침
	개선필요	개인정보처리방침을 수립하고 있으나 필수 8항목 중 일부항목이 누락되었음	
	취약	개인정보처리방침 미수립	

3.7.2	개인정보처리방침을 홈페이지 등에 공개하고 있는가?		35
설명	홈페이지를 운영하는 약국의 경우 개인정보처리방침(필수 8항목)을 홈페이지에 공개하고 홈페이지 미운영의 경우에는 고객(환자)이 인지할 수 있는 곳(처방전 접수대 등)에 비치하고 있는지 확인		
가이드	이행여부	운영현황	첨부파일
	양호	개인정보처리방침을 공개하고 있음	개인정보처리방침
	취약	개인정보처리방침 미공개	

3.8.1	개인정보보호책임자가 지정되고 그 역할이 정의되어 있는가?		36
설명	반드시 지정해야 할 개인정보보호책임자를 지정하고 있는 지 확인 ※ 개인정보보호책임자 지정 요건		

	<ul style="list-style-type: none"> ▶ 사업주 또는 대표자로 약국의 경우 약국장 ▶ 고객(환자)의 개인정보 보호업무를 위해 조직된 부서의 장 또는 개인정보보호에 관한 소양이 있는 사람 <p>※ 1인 약국은 약국장이 책임자/담당자/취급자가 됨</p>		
가이드	이행여부	운영현황	첨부파일
	양호	개인정보보호책임자를 지정하여 개인정보처리방침에 반영하고 있음	개인정보처리방침 또는 내부관리계획서
	취약	개인정보보호책임자 미지정	

3.8.2	개인정보 전담조직과 적정인력을 운영하고 있는가? (상시 근무인력이 5인 이상인 약국 해당)		37
설명	개인정보보호활동을 수행하는 전담조직과 적정인력(약국의 경우 전담인력 1명 이상)을 운영하는지 확인하는 사항으로 상시 근무인력이 5인 이상 약국에 해당됨		
가이드	이행여부	운영현황	첨부파일
	양호	전담조직과 적정인력을 운영하고 있음	조직구성표 또는 업무분장표
	취약	전담조직과 적정인력이 없음	
	해당사항 없음	1 ~ 4인 약국	

3.8.3	개인정보책임자가 교육 및 관리감독 등 역할을 수행하고 있는가?		38
설명	개인정보보호책임자(약국장 또는 약국장이 지정한 전담직원)는 1회/년 정기적으로 전문교육, 약사연수교육 시 개인정보보호 교육, 사이버교육(개인정보보호포탈, http://www.privacy.go.kr)을 이수하고 있는지 확인 ※ 개인정보보호책임자 교육은 일반직원 대상 직장교육은 인정하지 않음		

가이드	이행여부	운영현황	첨부파일
	양호	개인정보책임자가 교육 및 관리감독의 역할을 수행하고 있음	교육결과(교육이수 증빙)
	취약	교육 및 관리감독 역할 미수행	

3.8.4	개인정보보호 활동을 수행하는데 필요한 예산을 반영하고 있는가?		39
설명	개인정보보호를 위하여 1.교육 2.관리·감독 3.보안프로그램 도입(운영) 4.백신SW 도입(운영)에 소요된 비용을 책정하고 있는지 확인		
가이드	이행여부	운영현황	첨부파일
	양호	개인정보보호를 위해 필요한 예산을 반영하고 있음	
	취약	예산 반영이 없음	

3.9.1	개인정보 노출방지를 위한 모니터링 및 정기점검을 실시하고 있는가?		40
설명	회원가입이 필요한 홈페이지를 운영하는 약국 또는 PC내 저장된 개인정보의 노출방지를 위하여 점검프로그램(또는 보안프로그램) 등을 이용하여 검사 등 모니터링, 정기점검을 하는지 확인 ※ 홈페이지 개인정보 노출 진단 : 한국인터넷진흥원/개인정보보호포털에서 제공하는 개인정보 노출 진단서비스		
가이드	이행여부	운영현황	첨부파일
	양호	모니터링 및 정기점검으로 취약점에 대한 후속조치를 취하고 있음	개인정보 노출 점검리포트
	취약	개인정보 노출 점검을 하지 않고 있음	
	해당사항 없음	홈페이지를 운영하지 않거나 보안프로그램 미설치	

IV. 기타 주요 점검사항

약국관리프로그램(개인정보처리시스템)의 안전성 확보에 관한사항

⇨ 프로그램 제공업체에 해당기능 탑재 여부 확인(필수)

<p>✓ 접근권한 관리</p>	<p>약국관리프로그램 사용자가 1인 이상일 때 사용자에게 따라 약국관리프로그램 로그인 아이디/비밀번호 차등 부여</p>
<p>✓ 접근권한의 부여·변경·말소내역 기록·관리</p>	<p>약국관리프로그램 사용자의 접근권한 부여·변경·말소 내역은 최소 3년 보관</p>
<p>✓ 주민등록번호 암호화</p>	<p>약국관리프로그램 데이터베이스에 저장된 주민등록번호는 반드시 암호화 ⇨ 현재 PM2000, 유팜 등 약국관리프로그램의 전체 90%가 암호화 완료</p>
<p>✓ 취급자의 접속기록 보관</p>	<p>약국관리프로그램 사용자의 접속기록은 최소 6개월 이상 보관</p>
<p>✓ 접속기록이 위·변조 및 도난·분실되지 않도록 안전하게 보관</p>	
<p>✓ 개인정보의 파기</p>	<p>약국관리프로그램에 저장된 보유기간이 경과한 개인정보(환자정보, 조제기록, 청구정보 등 전산데이터) 파기</p>