

Vereniging Nederlandse Zorg- en Veiligheidshuizen
Vrijlandstraat 33B
4337 EA Middelburg



Auditplan WGS en BGS raamwerk Zorg- en Veiligheidshuizen

Versie:1.0

Datum:28-7-2026

Inhoudsopgave

1	Inleiding	3
1.1	Doel	3
1.2	Scope	3
1.3	Begrippenlijst	4
2	Gefaseerde auditaanpak	6
2.1	Fase 0 - Voorbereiding en verbetering procesinrichting	6
2.2	Fase 1 – Proefaudit (opzet en bestaan)	6
2.3	Fase 2 – Interne audit (opzet, bestaan en werking)	7
2.4	Fase 3 – Externe audit	7
3	Auditaanpak	8
3.1	Methoden	8
3.2	Steekproefstrategie	8
4	Rapportage	10

1 Inleiding

1.1 Doel

In dit auditplan is de aanpak opgenomen voor het beoordelen van het voor de Zorg- en Veiligheidshuizen opgestelde normenkader, dat is afgeleid van de Wet gegevensverwerking door samenwerkingsverbanden (WGS) en het Besluit gegevensverwerking door samenwerkingsverbanden (BGS) binnen het Zorg- en Veiligheidshuis (ZVH). Dit auditplan sluit aan op het ontwikkelde WGS-normenkader en de bijbehorende handreiking. Het normenkader vertaalt relevante wettelijke vereisten naar concrete normen, beheersmaatregelen en toetsingswerkzaamheden.

Het doel van een WGS-audit is om vast te stellen in hoeverre beheersmaatregelen zijn vastgesteld (opzet), aantoonbaar aanwezig zijn (bestaan) en daadwerkelijk worden toegepast (werking). Daarnaast ondersteunt een WGS-audit het identificeren van verbeterpunten en het vergroten van de auditgereedheid van het ZVH.

1.2 Scope

De audit heeft betrekking op de WGS-verwerkingsactiviteiten die plaatsvinden binnen het Zorg- en Veiligheidshuis (ZVH). De beoordeling richt zich op de inrichting, uitvoering en beheersing van de processen, rollen, verantwoordelijkheden en systemen die worden gebruikt voor de verwerking van persoonsgegevens binnen de wettelijke kaders van de WGS en het BGS.

De scope omvat:

WGS-verwerkingsactiviteiten

- Casusoverleggen;
- Gegevensuitwisseling binnen het samenwerkingsverband;
- Gegevensverstrekking aan derden;
- Casusregistratie;
- Het proces rondom de Rechtmatigheidsadviescommissie (RAC).

Rollen en verantwoordelijkheden

- Vaste deelnemers van het ZVH;
- Incidentele deelnemers;
- Derde partijen die persoonsgegevens ontvangen of betrokken zijn bij gegevensverstrekking;
- Het ondersteunend bureau van het ZVH.

Relevante informatiesystemen

- Kedo;
- PGaX;
- Overige ondersteunende systemen die worden gebruikt voor de uitvoering van WGS-processen, zoals kantoorautomatisering, e-mailvoorzieningen en gedeelde opslagomgevingen, voor zover deze onderdeel uitmaken van de verwerking van persoonsgegevens binnen het ZVH.

Gegevenslevenscyclus De scope betreft de relevante onderdelen van de gegevenslevenscyclus van gegevens binnen de WGS-processen, waaronder:

- Verzamelen en registreren van gegevens;
- Gebruik en bespreking van gegevens binnen casusoverleggen;

- Gegevensuitwisseling tussen deelnemers;
- Gegevensverstrekking aan derden;
- Bewaren, archiveren en vernietigen van gegevens;
- Toezicht, monitoring en rechtmatigheidsbeoordeling binnen het RAC-proces.

Buiten scope

De audit richt zich niet op de volledige bedrijfsvoering van deelnemende organisaties. Alleen processen en systemen die direct betrokken zijn bij de uitvoering van WGS-gerelateerde activiteiten binnen het ZVH, de zogenaamde basistaken, vallen binnen de scope van deze audit. Zogeheten plustaken die door een ondersteunend bureau worden uitgevoerd, vallen buiten de scope van deze audit.

1.3 Begrippenlijst

BEGRIJP	DEFINITIE
AUDIT	Systematische en onafhankelijke beoordeling om vast te stellen in hoeverre wordt voldaan aan het normenkader en de onderliggende vereisten uit de WGS en het BGS.
AUDITPERIODE	De periode waarover de auditwerkzaamheden worden uitgevoerd en waaruit de steekproef wordt geselecteerd.
AANTOONBAARHEID	Het kunnen onderbouwen dat een beheersmaatregel is ingericht en aanwezig is door middel van documentatie, registraties of andere bewijsstukken.
BEHEERSMAATREGEL	Maatregel, proces, afspraak of werkwijze die is ingericht om te voldoen aan vereisten uit de WGS en het BGS.
BEVINDING	Constatering uit een audit die wijst op een afwijking, risico, verbeterpunt of positieve observatie.
BESTAAN	De mate waarin een beheersmaatregel aantoonbaar aanwezig is en met bewijsstukken kan worden onderbouwd.
EXTERNE AUDIT	Onafhankelijke beoordeling uitgevoerd door een externe auditor of andere onafhankelijke partij buiten het ZVH.
INTERNE AUDIT	Onafhankelijke beoordeling uitgevoerd binnen of in opdracht van het ZVH ter toetsing van het normenkader.
NORMENKADER	Verzameling van normen, beheersmaatregelen en toetsingscriteria waarmee naleving van de WGS en het BGS wordt beoordeeld.
OPZET	De wijze waarop een beheersmaatregel, proces of werkwijze is ingericht om aan de norm te voldoen.
POPULATIE	De volledige verzameling van dossiers, registraties, besluiten of transacties waarop een auditwerkzaamheid betrekking heeft.
PROEFAUDIT	Eerste beoordeling gericht op het toetsen van de opzet en het bestaan van beheersmaatregelen en het valideren van het normenkader.

RISICOGERICHTE AANPAK	Auditmethode waarbij extra aandacht wordt besteed aan processen of activiteiten met een verhoogd privacy- of rechtmatigheidsrisico.
STEEKPROEF	Selectie van dossiers, registraties of andere objecten uit een populatie die wordt onderzocht om een oordeel te vormen over de betreffende norm.
WGS	Wet gegevensverwerking door samenwerkingsverbanden.
BGS	Besluit gegevensverwerking door samenwerkingsverbanden.
WERKING	De mate waarin de beheersmaatregel gedurende de controleperiode aantoonbaar heeft gefunctioneerd en overeenkomstig de opzet in de praktijk is toegepast.
ZORG- EN VEILIGHEIDSHUIS (ZVH)	Samenwerkingsverband als bedoeld in hoofdstuk 2 van de WGS waarin deelnemers samenwerken rondom complexe zorg- en veiligheidsvraagstukken.

2 Gefaseerde auditaanpak

Om Zorg- en Veiligheidshuizen voldoende tijd te geven om processen verder in te richten en ervaring op te doen met het normenkader, wordt een gefaseerde auditaanpak gehanteerd. Deze aanpak vormt een streefbeeld voor de voorbereiding op de verplichte privacy-audit.

Gelet op de verplichting uit artikel 1.18 BGS om de eerste privacy-audit uiterlijk 1 maart 2027 uit te voeren, stellen wij de volgende gefaseerde aanpak voor:

- Fase 0 – Voorbereiding en verbetering procesinrichting (2026)
- Fase 1 – Proefaudit (najaar 2026)
 - o Gericht op het toetsen van de opzet en het bestaan van beheersmaatregelen en het identificeren van verbeterpunten.
- Fase 2 – Interne audit (Q4 2026 – begin 2027)
 - o Gericht op het toetsen van opzet, bestaan en werking en het opvolgen van bevindingen uit de proefaudit.
- Fase 3 – Onafhankelijke/ externe audit (Q1 2027 - uiterlijk 1 maart 2027)
 - o Uitvoering van de verplichte privacy-audit conform de WGS en het BGS. Daarna vindt de audit eens per vier jaar plaats.

2.1 Fase 0 - Voorbereiding en verbetering procesinrichting

Voorafgaand aan de proefaudit krijgen de Zorg- en Veiligheidshuizen de gelegenheid om de vereisten uit de WGS en het BGS te vertalen naar de eigen praktijk denk hierbij aan aanvullende factsheet opstellen en het IB-handboek opstellen. Deze fase staat in het teken van het inrichten, formaliseren en aantoonbaar maken van de benodigde beheersmaatregelen, zodat een solide basis ontstaat voor de daaropvolgende auditfasen.

Doelstellingen:

- Implementeren van de beheersmaatregelen uit het normenkader;
- Inrichten en actualiseren van processen, procedures, werkinstructies en registraties;
- Vastleggen van rollen, verantwoordelijkheden en besluitvorming;
- Verzamelen en structureren van bewijsstukken die benodigd zijn voor toekomstige audits;
- Vergroten van kennis en bewustwording bij betrokken medewerkers en deelnemers;
- Identificeren en oplossen van eventuele hiaten voordat de proefaudit wordt uitgevoerd.

Deze fase is gericht op het vergroten van de auditgereedheid van het Zorg- en Veiligheidshuis en het creëren van voldoende aantoonbaarheid om de opzet, het bestaan en uiteindelijk de werking van de beheersmaatregelen te kunnen beoordelen.

2.2 Fase 1 – Proefaudit (opzet en bestaan)

De proefaudit richt zich op het beoordelen van de opzet en het bestaan van de beheersmaatregelen uit het normenkader.

Doelstellingen:

- Valideren van de praktische toepasbaarheid van het normenkader;
- Beoordelen of processen, procedures en afspraken zijn ingericht;

- Onderzoeken of er nog algemene wensen zijn voor de pakketten in het kader van de aantoonbaarheid;
- Identificeren van normen die voor meerdere ZVH's vergelijkbare bewijsstukken en toetsingswerkzaamheden kennen;

Signaleren van verbeterpunten ter voorbereiding op een interne audit.

De uitkomsten worden gebruikt om het normenkader en de handreiking waar nodig verder te verfijnen.

2.3 Fase 2 – Interne audit (opzet, bestaan en werking)

Na uitvoering van verbetermaatregelen wordt een interne audit uitgevoerd.

Doelstellingen:

- Beoordelen van opzet, bestaan en werking van de beheersmaatregelen;
- Vaststellen of maatregelen structureel worden toegepast;
- Identificeren van resterende bevindingen en verbeteracties;
- Vergroten van de auditgereedheid voor een externe audit.

De interne audit kan worden uitgevoerd door een onafhankelijke medewerker, privacyfunctionaris of andere aangewezen beoordelaar.

2.4 Fase 3 – Externe audit

De externe audit vormt de onafhankelijke beoordeling van de naleving van het normenkader door een externe auditor.

Doelstellingen:

- Vaststellen of het ZVH voldoet aan de relevante vereisten uit de WGS en het BGS;
- Beoordelen van de opzet, het bestaan en de werking van de beheersmaatregelen;
- Verstrekken van inzicht in resterende risico's en verbeterpunten;
- Onderbouwen van de naleving richting stakeholders en toezichthouders.

3 Auditaanpak

3.1 Methoden

De auditwerkzaamheden worden uitgevoerd overeenkomstig de testaanpak die is opgenomen bij het normenkader. Per norm is aangegeven hoe deze wordt beoordeeld: of de beheersmaatregel adequaat is ingericht, aantoonbaar aanwezig is en (indien van toepassing) effectief werkt.

De volgende onderzoekstechnieken worden toegepast:

- Documentreview van beleid, procedures, werkinstructies en registraties;
- Interviews met proceseigenaren, procesregisseurs en overige betrokken functionarissen;
- Inspectie van besluiten, verslagen, registers en overige bewijsstukken;
- Steekproeven op registraties, casusdossiers en uitgevoerde werkzaamheden.

Deze methoden sluiten aan bij de handreiking voor het beoordelen van opzet, bestaan en werking.

3.2 Steekproefstrategie

De audit maakt gebruik van een risicogerichte steekproefaanpak. Hierbij wordt een selectie gemaakt uit een afgebakende populatie van dossiers, registraties, besluiten of transacties waarop een norm betrekking heeft.

Populatie

Onder de populatie wordt verstaan de volledige verzameling van objecten waarop de controle betrekking heeft gedurende de geselecteerde auditperiode. Voorbeelden hiervan zijn:

- Alle casusdossiers die in de auditperiode zijn behandeld;
- Alle verstrekkingen aan derden;
- Alle RAC-beoordelingen;
- Alle autorisatieverzoeken;
- Alle geregistreeerde datalekken;
- Alle AVG-verzoeken van betrokkenen.

De auditor stelt vooraf per norm vast welke populatie relevant is voor de beoordeling.

Selectie van de steekproef

De steekproef wordt zoveel mogelijk willekeurig geselecteerd uit de vastgestelde populatie. Indien sprake is van verhoogde risico's of specifieke aandachtspunten kan aanvullend een gerichte selectie worden gemaakt, bijvoorbeeld voor:

- Verstrekkingen aan derden;
- Casussen waarbij incidentele deelnemers zijn betrokken;
- Uitzonderingssituaties of afwijkingen van de standaard werkwijze.

Omvang van de steekproef

De omvang van de steekproef is afhankelijk van de grootte van de populatie en het risico van het betreffende proces. Als richtlijn kan onderstaande staffel worden gehanteerd:

Populatie	Steekproef
1 t/m 50	Maximum 5 dossiers

51 t/m 250	10% - maximum 25 dossiers
250+	Maximum 25 dossiers

Indien de populatie uit minder dan vijf voorkomens bestaat, wordt 100% van de populatie geselecteerd. Voor processen met een verhoogd privacy- of rechtmatigheidsrisico kan de steekproef worden uitgebreid.

Geen waarnemingen beschikbaar

Indien gedurende de auditperiode geen dossiers, verstrekkingen of registraties beschikbaar zijn voor beoordeling, wordt dit vastgelegd als een auditwaarneming. In dat geval wordt uitsluitend beoordeeld of de opzet en het bestaan van de beheersmaatregelen voldoende zijn ingericht en aantoonbaar aanwezig zijn.

4 Rapportage

De bevindingen worden vastgelegd in een auditrapport.

Per norm wordt gerapporteerd:

- De uitgevoerde werkzaamheden;
- Het oordeel over opzet, bestaan en werking;
- De onderliggende bevindingen;
- Eventuele risico's;
- Verbetermaatregelen en aanbevelingen.

Bevindingen worden geclassificeerd op basis van impact en risico. Het auditrapport vormt de basis voor opvolging van verbetermaatregelen en voor eventuele vervolgbeoordelingen.

De auditresultaten kunnen daarnaast worden gebruikt voor zelfevaluaties, interne controles, verbetertrajecten en toekomstige externe audits

De voorgestelde rapportagevorm is gebaseerd op de huidige inzichten en wettelijke vereisten. Omdat de Autoriteit Persoonsgegevens (AP) nog geen nadere invulling heeft gegeven aan de rapportage-eisen onder de WGS en het BGS, kan deze rapportagevorm in de toekomst worden aangepast indien nieuwe richtlijnen of verwachtingen vanuit de AP daartoe aanleiding geven.